(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年10 月20 日 (20.10.2005)

PCT

(10) 国際公開番号
WO 2005/098795 A1

(51) 国際特許分類[7]: G09C 1/00, G06F 7/50

(21) 国際出願番号: PCT/JP2005/005136

(22) 国際出願日: 2005 年3 月22 日 (22.03.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2004-107778 2004 年3 月31 日 (31.03.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO.,LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真１００６番地 Osaka (JP).

(71) 出願人 (米国についてのみ): 山道 正美 (YAMAMICHI, Masami) (発明者(死亡)の相続人).

(72) 発明者: 山道 将人 (YAMAMICHI, Masato) (死亡).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 布田 裕一 (FUTA, Yuichi). 大森 基司 (OHMORI, Motoji). 静谷 啓樹 (SHIZUYA, Hiroyuki). 満保 雅浩 (MAMBO, Masahiro).

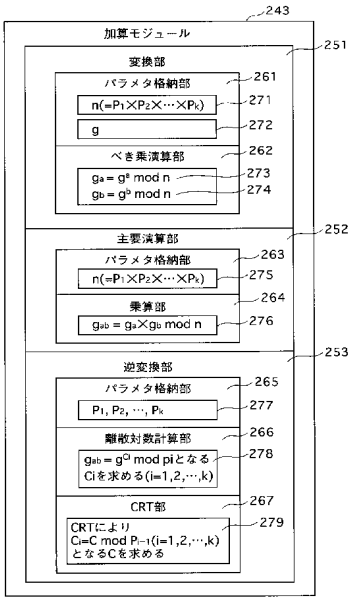
(74) 代理人: 中島 司朗, 外(NAKAJIMA, Shiro et al.); 〒5310072 大阪府大阪市北区豊崎三丁目２番１号淀川５番館６Ｆ Osaka (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU,

/続葉有/

(54) Title: COMPUTER SYSTEM, COMPUTER PROGRAM, AND ADDITION METHOD

(54) 発明の名称: 整数を加算するコンピュータシステム



243... ADDITION MODULE
251... CONVERSION UNIT
261... PARAMETER STORAGE UNIT
262... POWER CALCULATION UNIT
252... MAIN CALCULATION UNIT
263... PARAMETER STORAGE UNIT
264... MULTIPLICATION UNIT
253... INVERSE CONVERSION UNIT
265... PARAMETER STORAGE UNIT
266... DISCRETE LOGARITHM CALCULATION UNIT
278... CALCULATE Ci (i = 1, 2, ···, k) WHICH SATISFIES $g_{ab} = g^{Ci} \bmod pi$
267... CRT UNIT
279... CALCULATE C WHICH SATISFIES Ci = C mod Pi-1 (i = 1, 2, ···, k) BY CRT

(57) Abstract: There is provided a computer system which makes it difficult to analyze a calculation content. A power calculation unit (262) performs the following calculation for the input data "a" and "b": $g_a = g^a \bmod n$, $g_b = g^b \bmod n$. Next, a multiplication unit (264) performs the following calculation for g_a and g_b: $g_{ab} = g_a \times g_b \bmod n$. Next, a discrete logarithm calculation unit (266) calculates $c_i \bmod p_i - 1$ which satisfies $g_{ab} = g^{ci} \bmod p_i$ (i = 1, 2, ···, k). Next, a CRT unit (267) calculates "c" which satisfies $c_i = c \bmod p_i - 1$ (i = 1, 2, ···, k) by the Chinese remainder theorem (CRT).

(57) 要約: 演算の内容を解析しにくくするコンピュータシステムを提供する。 べき乗演算部２６２は、入力データａ、ｂに対し、 $g_a = g^a \bmod n$, $g_b = g^b \bmod n$を計算する。 次に、乗算部２６４は、g_a及びg_bに対し、 $g_{ab} = g_a \times g_b \bmod n$を計算する。 次に、離散対数計算部２６６は、 $g_{ab} = g^{ci} \bmod p_i$（ｉ＝１，２，…，ｋ）となるｃ$_i$ ｍｏｄ ｐ$_i$－１を求める。 次に、ＣＲＴ部２６７は、中国人剰余定理（ＣＲＴ）により、ｃ$_i$＝ｃ ｍｏｄ ｐ$_i$－１（ｉ＝１，２，…，ｋ）となるｃを求める。

WO 2005/098795 A1

ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書
— 請求の範囲の補正の期限前の公開であり、補正書受領 の際には再公開される。

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

整数を加算するコンピュータシステム

技術分野

[0001] 本発明は、コンピュータプログラムの解析を困難にする耐タンパーソフト技術に関する。

背景技術

[0002] 従来より、コンピュータプログラムに従って動作するプロセッサを備えるコンピュータシステムにおいて、秘密の通信や相手の認証をする際に、暗号プログラム(暗号ソフトウェア)が用いられる。

このとき、鍵や暗号アルゴリズムなどを含む暗号ソフトウェアをコンピュータシステムにそのまま実装すると、実装された暗号ソフトウェアを解析された場合に、簡単に不正な使用がされてしまう。このような問題点を解決するために、特許文献1は、演算及びデータの領域を変換することにより、元の演算及びデータを推測困難にする技術を開示している。

[0003] 例えば、入力データa、bに対し、加算を施して、加算結果a+bを出力する加算プログラムを想定する。

予め、整数k_1、k_2を保持し、これらを用いて、入力データa、bを、それぞれ$t_a = k_1 \times a + k_2$, $t_b = k_1 \times b + k_2$に変換する。ここで、「×」は、乗算を示す演算子である。

[0004] 次にt_a, t_bに対して、$t_{ab} = t_a + t_b$を計算する。

さらに、t_{ab}に対して、$c = (t_{ab} - 2k_2) / k_1$を計算する。

次に、演算結果cを出力する。

上記のように処理すると、

$$t_{ab} = t_a + t_b$$
$$= k_1 \times a + k_2 + k_1 \times b + k_2$$
$$= k_1 \times (a + b) + 2k_2$$ より、

$(t_{ab} - 2k_2) / k_1 = a + b$が成り立つ。

[0005] 従って、c=a+bとなり、加算プログラムによりaとbの加算結果が得られる。

特許文献1:米国特許第6594761号公報

特許文献2:日本国特許第3402441号特許公報

特許文献3:日本国特許第2760799号特許公報

非特許文献1:岡本龍明、山本博資、「現代暗号」、産業図書(1997年)

非特許文献2:Henri Cohen, "A Course in Computational Algebraic Number Theory", GTM 138, Springer-Verlag, 1993, pp.19-20

非特許文献3:I. Blake, G. Seroussi and N. Smart, "Elliptic Curves in Cryptography", CAMBRIDGE UNIVERSITY PRESS, 1999

非特許文献4:N. Kunihiro and K. Koyama, "Two Discrete Log Algorithms for Super-Anomalous Elliptic Curves", SCIS'99, 1999, pp. 869-874

発明の開示

発明が解決しようとする課題

[0006] 上記従来例の方式によると、変換後の領域においても通常の加算と同じ加算を行うため、変換後の演算を解析することにより、変換前の演算が加算であることが推測される可能性があるという問題点がある。プログラムにおいて、加算をしている箇所が、解析者により知られた場合に、その前後の部分がさらに集中して解析されると、どのような変換を行っているか知られてしまう恐れがある。ゆえに、可能な限り、変換前の演算を知られないようにした方がよい。

[0007] 本発明は、演算の内容を解析しにくくすることができるコンピュータシステム、コンピュータプログラム、加算方法及び記録媒体を提供することを目的とする。

課題を解決するための手段

[0008] 上記目的を達成するために、本発明は、2個以上の整数を加算するコンピュータシステムであって、複数のコンピュータ命令が組み合わされて構成されるコンピュータプログラムを記憶しているメモリ部と、前記記憶手段に記憶されている前記コンピュータプログラムから1個ずつコンピュータ命令を読み出し、解読し、その解読結果に応じて動作するプロセッサとを備え、前記コンピュータプログラムは、各整数に、群G上の冪演算を施すことにより、群Gに属する元を生成する変換命令群と、生成された全ての前記元に対して、前記加算とは異なる群G上の基本演算を施して、演算値を生成す

る演算命令群と、群G又は群Gに真に含まれる部分群Sにおいて、前記演算値に対して、前記変換命令群により施される冪演算の逆算を施すことにより、前記整数の加算値を生成する逆変換命令群とを含むことを特徴とする。

発明の効果

[0009] この構成によると、演算に使用する値の隠蔽だけでなく、演算そのものを隠蔽することができる。

ここで、前記コンピュータシステムは、対象情報を安全かつ確実に扱う情報セキュリティ装置であって、前記コンピュータプログラムは、さらに、対象情報にセキュリティ処理を施すセキュリティ命令群を含み、前記セキュリティ命令群は、加算演算において、前記変換命令群、前記演算命令群及び前記逆変換命令群を用いるとしてもよい。

[0010] この構成によると、セキュリティ処理における加算において、使用する値及び演算を隠蔽することができる。

ここで、前記群Gは、剰余整数環の乗法群であり、前記変換命令群は、各整数に冪乗を施し、演算命令群は、前記元に対して、乗算を施すとしてもよい。

この構成によると、変換後に施される演算は、乗算であり、加算と異なるので、演算を隠蔽することができる。

[0011] ここで、前記群Gは、2つの素数p，qと正整数mを用いて表される$n=p^m \times q$に対し、Z／nZの乗法群であり、前記変換命令群は、各整数に冪乗を施し、演算命令群は、前記元に対して、乗算を施すとしてもよい。

この構成によると、変換後に施される演算は、乗算であり、加算と異なるので、演算を隠蔽することができる。

[0012] ここで、前記部分群Sは、アノマラス楕円曲線の群であり、前記変換命令群は、各整数に楕円曲線上の乗算を施し、演算命令群は、前記元に対して、楕円曲線上の加算を施すとしてもよい。また、前記群Gは、二つのアノマラス楕円曲線の群の直積であり、前記変換命令群は、各整数に楕円曲線上の乗算を施し、演算命令群は、前記元に対して、楕円曲線上の加算を施すとしてもよい。

[0013] これらの構成によると、変換後に施される演算は、楕円曲線上の加算であり、整数の加算と異なるので、演算を隠蔽することができる。

ここで、さらに、前記逆変換命令群は、複数の冪数と、各冪数による冪乗値又は冪倍値とを対応付けて記憶しており、その対応付けを検索することにより、冪演算の逆算を求めるとしてもよい。

[0014] この構成によると、逆変換命令群による逆算が容易である。

ここで、前記情報セキュリティ装置は、鍵情報に基づいて対象情報を暗号化し又は復号し、前記セキュリティ命令群は、前記鍵情報に基づいて、対象情報を暗号化し又は復号し、暗号化又は復号において、鍵情報又は鍵情報から得られる二次鍵情報と、対象情報又は対象情報から得られる二次対象情報との加算演算が含まれ、前記加算演算において、前記変換命令群、前記演算命令群及び前記逆変換命令群を用いて、鍵情報又は鍵情報から得られる二次鍵情報と、対象情報又は対象情報から得られる二次対象情報とに、加算を施すとしてもよい。

[0015] この構成によると、暗号化又は復号における加算において、使用する値及び演算を隠蔽することができる。

ここで、前記情報セキュリティ装置は、鍵情報に基づいて対象情報にデジタル署名を施し又は署名検証を施し、前記セキュリティ命令群は、前記鍵情報に基づいて、対象情報にデジタル署名を施し又は署名検証を施し、デジタル署名又は署名検証において、鍵情報又は鍵情報から得られる二次鍵情報と、対象情報又は対象情報から得られる二次対象情報との加算演算が含まれ、前記加算演算において、前記変換命令群、前記演算命令群及び前記逆変換命令群を用いて、鍵情報又は鍵情報から得られる二次鍵情報と、対象情報又は対象情報から得られる二次対象情報とに、加算を施すとしてもよい。

[0016] この構成によると、デジタル署名又は署名検証における加算において、使用する値及び演算を隠蔽することができる。

以上説明したように、本発明の構成によると、演算に使用する値の隠蔽だけでなく、演算そのものを隠蔽することができ、その価値は大きい。

図面の簡単な説明

[0017] [図1]コンテンツ配信システム10の構成を示す構成図である。

[図2]コンテンツサーバ装置100の構成を示すブロック図である。

[図3]コンテンツ配信プログラム131の内容を説明するフローチャートである。

[図4]コンテンツ暗号プログラム132の内容を説明するフローチャートである。

[図5]暗号プログラム133の構成を示す構成図である。

[図6]暗号制御モジュール141の内容を説明するフローチャートである。図7へ続く。

[図7]暗号制御モジュール141の内容を説明するフローチャートである。図6から続く。

[図8]パーソナルコンピュータ200の構成を示すブロック図である。

[図9]コンテンツ受信プログラム231の内容を説明するフローチャートである。

[図10]コンテンツ復号プログラム232の内容を説明するフローチャートである。

[図11]復号プログラム234の構成を示す構成図である。

[図12]復号制御モジュール241の内容を説明するフローチャートである。図13へ続く。

[図13]復号制御モジュール241の内容を説明するフローチャートである。図12から続く。

[図14]加算モジュール243の構成を示す構成図である。

[図15]加算モジュール243による加算の動作を示すフローチャートである。

[図16]加算モジュール501の構成を示す構成図である。

[図17]加算モジュール501による加算の動作を示すフローチャートである。

[図18]加算モジュール601の構成を示す構成図である。

[図19]加算モジュール601による加算の動作を示すフローチャートである。

発明を実施するための最良の形態

[0018] 1．コンテンツ配信システム10

本発明に係る第1の実施の形態としてのコンテンツ配信システム10について説明する。

1．1 コンテンツ配信システム10の構成

コンテンツ配信システム10は、図1に示すように、コンテンツサーバ装置100、配信サーバ装置300a、放送装置300b、BD製造装置300c、パーソナルコンピュータ200、デジタル放送受信装置200a及びBD再生装置200bから構成されている。

[0019] コンテンツサーバ装置100は、映像データ及び音データから構成される映画のコンテンツを記憶しており、配信サーバ装置300aからの要求に応じて、記憶しているコンテンツを暗号化して暗号化コンテンツを生成し、生成した暗号化コンテンツを専用回線21を介して接続されている配信サーバ装置300aへ送信する。配信サーバ装置300aは、暗号化コンテンツを受信し、インターネット20を介して接続されているパーソナルコンピュータ200へ暗号化コンテンツを送信する。パーソナルコンピュータ200は、暗号化コンテンツを受信し、受信した暗号化コンテンツを復号して復号コンテンツを生成し、生成した復号コンテンツを再生して映像及び音を出力する。

[0020] また、コンテンツサーバ装置100は、上記と同様に、放送装置300bからの要求に応じて、暗号化コンテンツを生成し、生成した暗号化コンテンツを専用回線22を介して接続されている放送装置300bへ送信する。放送装置300bは、暗号化コンテンツを受信し、受信した暗号化コンテンツを放送波に乗せて放送し、デジタル放送受信装置200aは、放送波を受信し、受信した放送波から前記暗号化コンテンツを抽出し、抽出した暗号化コンテンツを復号して復号コンテンツを生成し、生成した復号コンテンツを再生して映像及び音を出力する。

[0021] さらに、コンテンツサーバ装置100は、上記と同様に、BD製造装置300cからの要求に応じて、暗号化コンテンツを生成し、生成した暗号化コンテンツを専用回線23を介して接続されているBD製造装置300cへ送信する。BD製造装置300cは、暗号化コンテンツを受信し、受信した暗号化コンテンツを記録媒体400に書き込む。暗号化コンテンツが書き込まれた記録媒体400は、販売されて利用者が購入する。利用者により、記録媒体400が装着されたBD再生装置200bは、記録媒体400から前記暗号化コンテンツを読み出し、読み出した暗号化コンテンツを復号して復号コンテンツを生成し、生成した復号コンテンツを再生して映像及び音を出力する。

[0022] 1．2 コンテンツサーバ装置100

コンテンツサーバ装置100は、図2に示すように、マイクロプロセッサ101、ハードディスク部102、メモリ部103、入力制御部104、表示制御部105及び通信ユニット106などから構成されるコンピュータシステムである。入力制御部104及び表示制御部105は、それぞれ、キーボード107及びモニタ108に接続されている。また、通信ユニッ

ト106は、専用回線21、22及び23を介して、それぞれ、配信サーバ装置300a、放送装置300b及びBD製造装置300cに接続されている。

[0023] ハードディスク部102及びメモリ部103には、様々なコンピュータプログラムが記憶されており、マイクロプロセッサ101が、前記コンピュータプログラムに従って動作することにより、コンテンツサーバ装置100は、その一部の機能を達成する。

(1)ハードディスク部102

ハードディスク部102は、図2に示すように、コンテンツ120、コンテンツ121、コンテンツ122、・・・、鍵123、鍵124、鍵125、・・・、及び図示していないその他のコンピュータプログラムを記憶している。また、暗号化コンテンツ126、暗号化コンテンツ127、暗号化コンテンツ128、・・・を記憶するための領域を備えている。

[0024] コンテンツ120、コンテンツ121、コンテンツ122、・・・は、それぞれ、鍵123、鍵124、鍵125、・・・、に対応しており、また、暗号化コンテンツ126、暗号化コンテンツ127、暗号化コンテンツ128、・・・に対応している。

コンテンツ120、コンテンツ121、コンテンツ122、・・・は、それぞれ、映像データ及び音データが高効率に圧縮符号化された圧縮データである。

[0025] 鍵123、鍵124、鍵125、・・・は、それぞれ、コンテンツ120、コンテンツ121、コンテンツ122、・・・に、暗号化アルゴリズムを施して、暗号化コンテンツ126、暗号化コンテンツ127、暗号化コンテンツ128、・・・を生成する際に使用される暗号鍵であり、それぞれ、64ビット長のデータである。ここで、前記暗号化アルゴリズムについては、後述する。

[0026] 暗号化コンテンツ126、暗号化コンテンツ127、暗号化コンテンツ128、・・・は、それぞれ、コンテンツ120、コンテンツ121、コンテンツ122、・・・に、前記暗号化アルゴリズムが施されて生成された暗号化データである。

(2)メモリ部103

メモリ部103は、図2に示すように、コンテンツ配信プログラム131、コンテンツ暗号プログラム132、暗号プログラム133、送信プログラム134及び図示していないその他のプログラムを記憶している。これらのプログラムは、それぞれ、機械語形式の複数の命令コードを組み合わせて構成されるコンピュータプログラムである。前記機械語

形式は、マイクロプロセッサ101により解読され実行される形式である。

[0027] 以下において、各コンピュータプログラムの内容を説明するが、各コンピュータプログラムの内容の理解を容易にするために、機械語形式の命令コードを用いた表現ではなく、フローチャートにより各コンピュータプログラムの内容を表現し、フローチャートを用いて、各コンピュータプログラムを説明する。

(a)コンテンツ配信プログラム131

コンテンツ配信プログラム131は、図3に示すように、命令コード群S101、S102、S103及びS104を含んで構成されており、これらの命令コード群は、コンテンツ配信プログラム131内において、この順序で並べられている。各命令コード群は、1個又は複数個の命令コードを含んでいる。

[0028] 命令コード群S101は、コンテンツサーバ装置100の管理者からコンテンツの指定を受け付け、又はコンテンツの配信先の装置からコンテンツの指定を受け取ることを示す複数の命令コードを含む。

命令コード群S102は、コンテンツの配信先の装置の指定を受け取ることを示す複数の命令コードを含む。

[0029] 命令コード群S103は、受け付けた指定又は受け取った指定により示されるコンテンツを指定して、コンテンツ暗号プログラム132を呼び出し、次に、コンテンツ暗号プログラム132により生成された暗号化コンテンツを暗号化コンテンツ126としてハードディスク部102へ書き込むことを示す複数の命令コードを含む。

命令コード群S104は、受け取った指定による配信先の装置と、生成されハードディスク部102に書き込まれた暗号化コンテンツとを指定して、送信プログラム134を呼び出すことを示す複数の命令コードを含む。命令コード群S104が実行されることにより、受け取った指定により示される配信先の装置へ、生成された暗号化コンテンツが送信される。

[0030] (b)コンテンツ暗号プログラム132

コンテンツ暗号プログラム132は、図4に示すように、命令コード群S111、S112、S113、S114、S115及びS116を含んで構成されており、これらの命令コード群は、コンテンツ暗号プログラム132内において、この順序で並べられている。各命令コード

群は、1個又は複数個の命令コードを含んでいる。

[0031] 命令コード群S111は、指定を受け付けたコンテンツ内におけるデータの位置をビットにより示す読出しポイントに、初期値として値「−64」を代入し、指定を受け付けたコンテンツに対応する鍵をハードディスク部102から読み出すことを示す複数の命令コードを含む。ここで、値「−64」を有する読出しポイントは、前記コンテンツ外の位置を示しているが、読出しポイントに初期値として値「−64」を代入するのは、後述する命令コード群S112の最初の実行において、読出しポイントが、前記コンテンツの先頭の位置を示すようにするためである。後述する命令コード群S112の最初の実行において、前記読出しポイントに64ビットが加算され、読出しポイントは、値「0」を有することになり、この読出しポイントは、前記コンテンツの先頭の位置を示している。

[0032] 命令コード群S112は、前記読出しポイントに64ビットを加算し、次に、前記コンテンツにおいて、加算された読出しポイントにより示される位置から1ブロック分のデータの読出しを試みることを示す複数の命令コードと、読出しポイントにより示される位置が前記コンテンツ内であるならば、当該位置から1ブロック分のデータを読み出し、読出しポイントにより示される位置が前記コンテンツの外を示すならば、ブロックの読み出しが終了したことを示す終了コードを出力することを示す複数の命令コードとを含む。ここで、1ブロックは、64ビット長のデータである。

[0033] 命令コード群S113は、命令コード群S112から終了コードが出力された場合には、コンテンツ暗号プログラム132による処理を終了し、終了コードが出力されていない場合には、次の命令コード群S114に制御を移すことを示す複数の命令コードを含む。

命令コード群S114は、読み出された前記鍵及び読み出された前記1ブロックを伴って、暗号プログラム133を呼び出すことを示す複数の命令コードを含む。

[0034] 命令コード群S115は、暗号プログラム133により生成された1個の暗号化ブロックを、ハードディスク部102に対して、暗号化コンテンツ126の一部として書き込むことを示す複数の命令コードを含む。

命令コード群S116は、次に、制御を命令コード群S112へ移すことを示す命令コードを含む。

[0035] (c)暗号プログラム133

暗号プログラム133は、図5に示すように、暗号制御モジュール141、拡張鍵生成モジュール142及びローテーションモジュールA143、ローテーションモジュールB144、ローテーションモジュールC145及びローテーションモジュールD146から構成されている。

[0036] 各モジュールは、機械語形式の複数の命令コードを組み合わせて構成されるコンピュータプログラムである。前記機械語形式は、マイクロプロセッサ101により解読され実行される形式である。

(拡張鍵生成モジュール142)

拡張鍵生成モジュール142は、呼出し元のプログラムから、64ビットの鍵Kを受け取り、受け取った鍵Kを用いて、8個の拡張鍵K1、K2、K3、・・・、K8を生成し、生成した8個の拡張鍵K1、K2、K3、・・・、K8を呼出し元のプログラムへ出力する複数の命令コードを含む。

[0037] なお、拡張鍵を生成する方法については、特許文献3に記載されているため、説明を省略する。

(ローテーションモジュールA143)

ローテーションモジュールA143は、呼出し元のプログラムから32ビットのデータXを受け取り、データXに対して、Rot2(X)+X+1を演算し、演算結果を呼出し元のプログラムへ出力する複数の命令コードを含む。

[0038] ここで、Rot2(X)は、32ビットのデータXを左へ2ビット循環シフトすることを示す。なお、32ビットのデータXを左へ2ビット循環シフトするとは、データXを最上位2ビットX1と最下位30ビットX2に分け、X2を、データXの最上位30ビットにシフトし、X1をデータXの最下位2ビットにシフトすることを言う。

(ローテーションモジュールB144)

ローテーションモジュールB144は、呼出し元のプログラムから32ビットのデータXを受け取り、データXに対して、Rot4(X) XOR Xを演算し、演算結果を呼出し元のプログラムへ出力する複数の命令コードを含む。

[0039] ここで、Rot4(X)は、データXを左へ4ビット循環シフトすることを示し、XORは、排

他的論理和を示す。なお、32ビットのデータXを左へ4ビット循環シフトするとは、データXを最上位4ビットX1と最下位28ビットX2に分け、X2を、データXの最上位28ビットにシフトし、X1をデータXの最下位4ビットにシフトすることを言う。

[0040] （ローテーションモジュールC145）

ローテーションモジュールC145は、呼出し元のプログラムから32ビットのデータXを受け取り、データXに対して、Rot8（X） XOR Xを演算し、演算結果を呼出し元のプログラムへ出力する複数の命令コードを含む。

ここで、Rot8（X）は、データXを左へ8ビット循環シフトすることを示す。なお、32ビットのデータXを左へ8ビット循環シフトするとは、データXを最上位8ビットX1と最下位24ビットX2に分け、X2を、データXの最上位24ビットにシフトし、X1をデータXの最下位8ビットにシフトすることを言う。

[0041] （ローテーションモジュールD146）

ローテーションモジュールD146は、呼出し元のプログラムから32ビットのデータX及び32ビットのデータYを受け取り、データX及びデータYに対して、Rot16（X）＋（X AND Y）を演算し、演算結果を呼出し元のプログラムへ出力する複数の命令コードを含む。

[0042] ここで、Rot16（X）は、データXを、左へ16ビット循環シフトすることを示し、ANDは、論理積を示す。なお、32ビットのデータXを左へ16ビット循環シフトするとは、データXを最上位16ビットX1と最下位16ビットX2に分け、X2を、データXの最上位16ビットにシフトし、X1をデータXの最下位16ビットにシフトすることを言う。

[0043] （暗号制御モジュール141）

暗号制御モジュール141は、図6及び図7に示すように、命令コード群S121ー命令コード群S140を含んで構成されており、これらの命令コード群は、暗号制御モジュール141内において、この順序で並べられている。各命令コード群は、1個又は複数個の命令コードを含む。

[0044] 命令コード群S121は、暗号制御モジュール141の呼出し元のプログラムから、1ブロックの平文M及び鍵Kを受け取ることを示す複数の命令コードを含む。ここで、1ブロックは、64ビット長のデータである。

命令コード群S122は、受け取った鍵Kを伴って、拡張鍵生成モジュール142を呼び出すことを示す複数の命令コードを含む。命令コード群S122が実行されると、その結果、8個の拡張鍵K1、K2、K3、・・・、K8が生成される。

[0045] 命令コード群S123は、データM1を定義する命令コード及びデータM2を定義する命令コードを含む。データM1は、受け取った平文Mの最上位の32ビットのデータであり、データM2は、受け取った平文Mの最下位の32ビットのデータである。

命令コード群S124は、データM1とデータM2とに排他的論理和XORを施し、その演算結果を変数TMP1に格納することを示す複数の命令コードを含む。

[0046] TMP1＝M1 XOR M2

命令コード群S125は、変数TMP1と拡張鍵K1とに加算を施し、その演算結果を変数TMP2に格納することを示す複数の命令コードを含む。

TMP2＝TMP1 ＋ K1

命令コード群S126は、変数TMP2を伴って、ローテーションモジュールA143を呼び出し、その演算結果を変数TMP3に格納することを示す複数の命令コードを含む。

[0047] TMP3＝Rot2(TMP2)＋TMP2＋1

命令コード群S127は、変数TMP3を伴って、ローテーションモジュールB144を呼び出し、その演算結果を変数TMP4に格納することを示す複数の命令コードを含む。

TMP4＝Rot4(TMP3) XOR TMP3

命令コード群S128は、変数TMP4とデータM1とに排他的論理和XORを施し、その演算結果を変数TMP5に格納することを示す複数の命令コードを含む。

[0048] TMP5＝TMP4 XOR M1

命令コード群S129は、変数TMP5と拡張鍵K2とに加算を施し、その演算結果を変数TMP6に格納することを示す複数の命令コードを含む。

TMP6＝TMP5 ＋ K2

命令コード群S130は、変数TMP6を伴って、ローテーションモジュールA143を呼び出し、その演算結果を変数TMP7に格納することを示す複数の命令コードを含む

。

[0049] TMP7＝Rot2(TMP6)＋TMP6＋1

命令コード群S131は、変数TMP7を伴って、ローテーションモジュールC145を呼び出し、その演算結果を変数TMP8に格納することを示す複数の命令コードを含む。

TMP8＝Rot8(TMP7) XOR TMP7

命令コード群S132は、変数TMP8と拡張鍵K3とに加算を施し、その演算結果を変数TMP9に格納することを示す複数の命令コードを含む。

[0050] TMP9＝TMP8 ＋ K3

命令コード群S133は、変数TMP9を伴って、ローテーションモジュールA143を呼び出し、その演算結果を変数TMP10に格納することを示す複数の命令コードを含む。

TMP10＝Rot2(TMP9)＋TMP9＋1

命令コード群S134は、変数TMP7及び変数TMP10を伴って、ローテーションモジュールD146を呼び出し、その演算結果を変数TMP11に格納することを示す複数の命令コードを含む。

[0051] TMP11＝Rot16(TMP10)＋(TMP10 AND TMP7)

命令コード群S135は、変数TMP11と変数TMP1とに排他的論理和XORを施し、その演算結果を変数TMP12に格納することを示す複数の命令コードを含む。

TMP12＝TMP11 XOR TMP1

命令コード群S136は、変数TMP12と拡張鍵K4とに加算を施し、その演算結果を変数TMP13に格納することを示す複数の命令コードを含む。

[0052] TMP13＝TMP12 ＋ K4

命令コード群S137は、変数TMP13を伴って、ローテーションモジュールA143を呼び出し、その演算結果を変数TMP14に格納することを示す複数の命令コードを含む。

TMP14＝Rot2(TMP13)＋TMP13＋1

命令コード群S138は、変数TMP14と変数TMP4とに排他的論理和XORを施し、

その演算結果を変数TMP15に格納することを示す複数の命令コードを含む。

[0053] TMP15＝TMP14 XOR TMP4

命令コード群S139は、変数TMP15と変数TMP12とに排他的論理和XORを施し、その演算結果を変数TMP16に格納することを示す複数の命令コードを含む。

TMP16＝TMP15 XOR TMP12

命令コード群S140は、変数TMP15を最上位32ビット、変数TMP16を最下位32ビットとする64ビットの整数を暗号文Cとして、呼出し元のプログラムへ出力することを示す複数の命令コードを含む。

[0054] (d)送信プログラム134

送信プログラム134(図示していない)は、複数の命令コードが並べられて構成されており、呼出し元のプログラムから、データの指定及び配信先の装置の指定を受け取り、通信ユニット106を制御して、指示されたデータを指定された配信先の装置へ送信することを示す複数の命令コードを含む。

[0055] 1．3 パーソナルコンピュータ200

パーソナルコンピュータ200は、図8に示すように、マイクロプロセッサ201、ハードディスク部202、メモリ部203、入力制御部204、表示制御部205及び通信ユニット206などから構成されるコンピュータシステムである。入力制御部204及び表示制御部205は、それぞれ、キーボード707及びモニタ208に接続されている。また、通信ユニット206は、インターネット20に接続されている。

[0056] ハードディスク部202及びメモリ部203には、様々なコンピュータプログラムが記憶されており、マイクロプロセッサ201が、各コンピュータプログラムに従って動作することにより、パーソナルコンピュータ200は、その一部の機能を達成する。

なお、デジタル放送受信装置200a及びBD再生装置200bは、パーソナルコンピュータ200と同様の構成を有しているので、これらの装置についての説明を省略する。

[0057] (1)ハードディスク部202

ハードディスク部202は、図8に示すように、鍵222を記憶しており、また暗号化コンテンツ221を記憶するための領域を備えている。暗号化コンテンツ221と鍵222とは、対応している。

暗号化コンテンツ221及び鍵222は、それぞれ、コンテンツサーバ装置100のハードディスク部102に記憶されている暗号化コンテンツ126及び鍵123と同じものである。

[0058] (2)メモリ部203

メモリ部203は、図8に示すように、コンテンツ受信プログラム231、コンテンツ復号プログラム232、再生プログラム233、復号プログラム234及び加算プログラム235を記憶している。また、メモリ部203は、復号コンテンツ領域236を含む。これらのプログラムは、それぞれ、機械語形式の複数の命令コードを組み合わせて構成されるコンピュータプログラムである。前記機械語形式は、マイクロプロセッサ201により解読され実行される形式である。

[0059] 復号コンテンツ領域236には、暗号化コンテンツが復号されて生成された復号コンテンツが一時的に書き込まれる。

以下において、各コンピュータプログラムの内容を説明するが、各コンピュータプログラムの内容の理解を容易にするために、機械語形式の命令コードを用いた表現ではなく、フローチャートにより各コンピュータプログラムの内容を表現し、フローチャートを用いて、各コンピュータプログラムを説明する。

[0060] (a)コンテンツ受信プログラム231

コンテンツ受信プログラム231は、図9に示すように、命令コード群S201、S202、S203及びS204を含んで構成されており、これらの命令コード群は、コンテンツ受信プログラム231内において、この順序で並べられている。各命令コード群は、1個又は複数個の命令コードを含んでいる。

[0061] 命令コード群S201は、パーソナルコンピュータ200の利用者からコンテンツの指定を受け付けることを示す複数の命令コードを含んでいる。

命令コード群S202は、指定を受け付けた前記コンテンツを識別するコンテンツ識別子を取得し、取得したコンテンツ識別子を、通信ユニット206及びインターネット20を介して、配信サーバ装置300aへ送信することを示す複数の命令コードを含んでいる。

[0062] 命令コード群S203は、配信サーバ装置300aから、インターネット20及び通信ユニ

ット206を介して、暗号化コンテンツを受信することを示す複数の命令コードを含んでいる。ここで、受信する前記暗号化コンテンツは、前記コンテンツ識別子により識別されるものである。

命令コード群S204は、受信した暗号化コンテンツをハードディスク部202へ、暗号化コンテンツ221として書き込むことを示す複数の命令コードを含んでいる。

[0063] (b)コンテンツ復号プログラム232

コンテンツ復号プログラム232は、図10に示すように、命令コード群S211、S212、S213、S214、S215、S216、S217及びS218を含んで構成されており、これらの命令コード群は、コンテンツ復号プログラム232内において、この順序で並べられている。各命令コード群は、1個又は複数個の命令コードを含んでいる。

[0064] 命令コード群S211は、パーソナルコンピュータ200の利用者から、ハードディスク部202に記憶されているいずれかの暗号化コンテンツの指定を受け付けることを示す複数の命令コードを含んでいる。

命令コード群S212は、メモリ部203に記憶されている再生プログラム233を呼び出すことを示す複数の命令コードを含んでいる。命令コード群S212が実行されることにより、その結果、コンテンツ復号プログラム232と再生プログラム233とが並行して実行される。

[0065] 命令コード群S213は、指定を受け付けた暗号化コンテンツ内におけるデータの位置をビットにより示す読出しポイントに初期値として値「−64」を代入し、次に、指定を受け付けた暗号化コンテンツに対応する鍵をハードディスク部202から読み出すことを示す複数の命令コードを含んでいる。

命令コード群S214は、前記読出しポイントに64ビットを加算し、次に、前記暗号化コンテンツにおいて、加算された読出しポイントにより示される位置から1ブロック分のデータの読出しを試みることを示す複数の命令コードと、読出しポイントにより示される位置が前記暗号化コンテンツ内であるならば、当該位置から1ブロック分のデータを読み出し、読出しポイントにより示される位置が前記暗号化コンテンツの外を示すならば、ブロックの読み出しが終了したことを示す終了コードを出力することを示す複数の命令コードとを含んでいる。ここで、1ブロックは、64ビット長のデータである。

[0066] 命令コード群S215は、命令コード群S214から終了コードが出力された場合には、コンテンツ復号プログラム232による処理を終了し、終了コードが出力されていない場合には、次の命令コード群S216に制御を移すことを示す複数の命令コードを含んでいる。

命令コード群S216は、読み出された前記鍵及び読み出された前記1ブロックを伴って、復号プログラム234を呼び出すことを示す複数の命令コードを含んでいる。

[0067] 命令コード群S217は、復号プログラム234により生成された1個の復号ブロックを、メモリ部203の復号コンテンツ領域236へ書き込むことを示す複数の命令コードを含んでいる。

命令コード群S218は、次に制御を命令コード群S214へ移すことを示す命令コードを含んでいる。

[0068] (c)再生プログラム233

再生プログラム233は、図10に示すように、命令コード群S218、S219及びS220を含んで構成されており、これらの命令コード群は、再生プログラム233は内において、この順序で並べられている。各命令コード群は、1個又は複数個の命令コードを含んでいる。

[0069] 命令コード群S218は、メモリ部203が有する復号コンテンツ領域236から1個以上の復号ブロックを読み出すことを示す複数の命令コードを含んでいる。

命令コード群S219は、読み出した前記復号ブロックから映像データ及び音データを生成し、生成した映像データ及び音データを映像信号及び音信号に変換して、表示制御部205を介して、モニタ208へ出力することを示す複数の命令コードを含んでいる。

[0070] 命令コード群S220は、次に制御を命令コード群S218へ移すことを示す命令コードを含んでいる。

(d)復号プログラム234

復号プログラム234は、図11に示すように、復号制御モジュール241、拡張鍵生成モジュール242、加算モジュール243、ローテーションモジュールA244、ローテーションモジュールB245、ローテーションモジュールC246及びローテーションモジュー

ルD247から構成されている。

[0071] 各モジュールは、機械語形式の複数の命令コードを組み合わせて構成されるコンピュータプログラムである。前記機械語形式は、マイクロプロセッサ201により解読され実行される形式である。

拡張鍵生成モジュール242、ローテーションモジュールA244、ローテーションモジュールB245、ローテーションモジュールC246及びローテーションモジュールD247は、それぞれ、図5に示す拡張鍵生成モジュール142、ローテーションモジュールA143、ローテーションモジュールB144、ローテーションモジュールC145及びローテーションモジュールD146と同じであるので、説明を省略する。

[0072] （復号制御モジュール241）

復号制御モジュール241は、図12及び図13に示すように、命令コード群S221ー命令コード群S240を含んで構成されており、これらの命令コード群は、復号制御モジュール241内において、この順序で並べられている。各命令コード群は、1個又は複数個の命令コードを含む。

[0073] 命令コード群S221は、復号制御モジュール241の呼出し元のプログラムから、1ブロックの暗号文M及び鍵Kを受け取ることを示す複数の命令コードを含む。ここで、1ブロックは、64ビット長のデータである。

命令コード群S222は、受け取った鍵Kを伴って、拡張鍵生成モジュール242を呼び出すことを示す複数の命令コードを含む。命令コード群S222が実行されると、その結果、8個の拡張鍵K1、K2、K3、・・・、K8が生成される。

[0074] 命令コード群S223は、データM1を定義する命令コード及びデータM2を定義する命令コードを含む。データM1は、受け取った暗号文Mの最上位の32ビットのデータであり、データM2は、受け取った暗号文Mの最下位の32ビットのデータである。

命令コード群S224は、データM1とデータM2とに排他的論理和XORを施し、その演算結果を変数TMP1に格納することを示す複数の命令コードを含む。

[0075] TMP1＝M1 XOR M2

命令コード群S225は、変数TMP1と拡張鍵K1とを伴って、加算モジュール243を呼び出し、その演算結果を変数TMP2に格納することを示す複数の命令コードを含

む。この結果、加算モジュール243により、TMP2＝TMP1 ＋ K1が算出される。

[0076] 命令コード群S226は、変数TMP2を伴って、ローテーションモジュールA244を呼び出し、その演算結果を変数TMP3に格納することを示す複数の命令コードを含む。

TMP3＝Rot2(TMP2)＋TMP2＋1

命令コード群S227は、変数TMP3を伴って、ローテーションモジュールB245を呼び出し、その演算結果を変数TMP4に格納することを示す複数の命令コードを含む。

[0077] TMP4＝Rot4(TMP3) XOR TMP3

命令コード群S228は、変数TMP4とデータM1とに排他的論理和XORを施し、その演算結果を変数TMP5に格納することを示す複数の命令コードを含む。

TMP5＝TMP4 XOR M1

命令コード群S229は、変数TMP5と拡張鍵K2とを伴って、加算モジュール243を呼び出し、その演算結果を変数TMP6に格納することを示す複数の命令コードを含む。この結果、加算モジュール243により、TMP6＝TMP5 ＋ K2が算出される。

[0078] 命令コード群S230は、変数TMP6を伴って、ローテーションモジュールA244を呼び出し、その演算結果を変数TMP7に格納することを示す複数の命令コードを含む。

TMP7＝Rot2(TMP6)＋TMP6＋1

命令コード群S231は、変数TMP7を伴って、ローテーションモジュールC246を呼び出し、その演算結果を変数TMP8に格納することを示す複数の命令コードを含む。

[0079] TMP8＝Rot8(TMP7) XOR TMP7

命令コード群S232は、変数TMP8と拡張鍵K3とを伴って、加算モジュール243を呼び出し、その演算結果を変数TMP9に格納することを示す複数の命令コードを含む。この結果、加算モジュール243により、TMP9＝TMP8 ＋ K3が算出される。

[0080] 命令コード群S233は、変数TMP9を伴って、ローテーションモジュールA244を呼び出し、その演算結果を変数TMP10に格納することを示す複数の命令コードを含

む。

TMP10＝Rot2（TMP9）＋TMP9＋1

命令コード群S234は、変数TMP7及び変数TMP10を伴って、ローテーションモジュールD247を呼び出し、その演算結果を変数TMP11に格納することを示す複数の命令コードを含む。

[0081] TMP11＝Rot16（TMP10）＋（TMP10 AND TMP7）

命令コード群S235は、変数TMP11と変数TMP1とに排他的論理和XORを施し、その演算結果を変数TMP12に格納することを示す複数の命令コードを含む。

TMP12＝TMP11 XOR TMP1

命令コード群S236は、変数TMP12と拡張鍵K4とを伴って、加算モジュール243を呼び出し、その演算結果を変数TMP13に格納することを示す複数の命令コードを含む。この結果、加算モジュール243により、TMP13＝TMP12 ＋ K4が算出される。

[0082] 命令コード群S237は、変数TMP13を伴って、ローテーションモジュールA244を呼び出し、その演算結果を変数TMP14に格納することを示す複数の命令コードを含む。

TMP14＝Rot2（TMP13）＋TMP13＋1

命令コード群S238は、変数TMP14と変数TMP4とに排他的論理和XORを施し、その演算結果を変数TMP15に格納することを示す複数の命令コードを含む。

[0083] TMP15＝TMP14 XOR TMP4

命令コード群S239は、変数TMP15と変数TMP12とに排他的論理和XORを施し、その演算結果を変数TMP16に格納することを示す複数の命令コードを含む。

TMP16＝TMP15 XOR TMP12

命令コード群S240は、変数TMP15を最上位32ビット、変数TMP16を最下位32ビットとする64ビットの整数を復号文Cとして、呼出し元のプログラムへ出力することを示す複数の命令コードを含む。

[0084] （加算モジュール243）

加算モジュール243は、入力データa、bに対し、データa＋bを演算し、データa＋b

を出力するコンピュータプログラムであり、図14に示すように、変換部251、主要演算部252及び逆変換部253から構成されており、変換部251は、パラメタ格納部261及びべき乗演算部262を含み、主要演算部252は、パラメタ格納部263及び乗算部264を含み、逆変換部253は、パラメタ格納部265、離散対数計算部266及びCRT(Chinese Remainder Theorem)部267を含む。

[0085] (i)各種パラメータ及び記号の定義、並びに入力データの条件

ここで、加算モジュール243で使用する各種パラメータ及び記号の定義、並びに入力データの条件について説明する。

p_i (i=1, 2, …, k)を、それぞれ異なる素数とする。例えば、p_i (i=1, 2, …, k)は、$p_1=3$、$p_2=5$、$p_3=7$、$p_4=13$、・・・などのように、それぞれ小さい素数である。また、例えば、k=17である。また、それらの積$p_1 \times p_2 \times \cdots \times p_k$をnとする。ここで、×は乗算を示す。nは、例えば、64ビット程度で表現できる数である。例えば、k=17のとき、$n=p_1 \times p_2 \times \cdots \times p_k > 2^{64}$となる。

[0086] p_i (i=1, 2, …, k)は、逆変換部253により保持され、nは、変換部251及び主要演算部252により保持されている。

加算モジュール243では、mod nの整数から構成される剰余整数環Z/nZの乗法群の演算を用いる。gは、その乗法群に属する予め与えられた数であり、p_i (i=1, 2, …, k)に対して原始元とする。

[0087] 原始元とは、mを1, 2, …と動かしたとき、初めて$g^m = 1 \mod p_i$となるmの値が、$p_i - 1$であるようなgである。

$L=LCM(p_1-1, p_2-1, \cdots, p_k-1)$とする。ここで、$LCM(p_1-1, p_2-1, \cdots, p_k-1)$は、$p_1-1, p_2-1, \cdots, p_k-1$の最小公倍数(Least Common Multiple)を示す。

[0088] 入力データa、bは、それぞれ、L/2より小さい非負整数とする。

(ii)変換部251の構成

変換部251は、パラメタ格納部261及びべき乗演算部262を含む。

パラメタ格納部261は、nとgとを格納している。

べき乗演算部262は、入力データa、bを受け取り、受け取った入力データa、bに対し、

$g_a = g^a \bmod n$, 及び

$g_b = g^b \bmod n$を計算し、得られたg_a及びg_bを主要演算部252へ出力する。

[0089] (iii)主要演算部252の構成

主要演算部252は、パラメタ格納部263及び乗算部264を含む。

パラメタ格納部263は、nを格納している。

乗算部264は、べき乗演算部262からg_a及びg_bを受け取り、受け取ったg_a及びg_bに対し、

$g_{ab} = g_a \times g_b \bmod n$を計算し、得られた$g_{ab}$を逆変換部253へ出力する。

[0090] (iv)逆変換部253の構成

逆変換部253は、パラメタ格納部265、離散対数計算部266及びCRT部267を含む。

パラメタ格納部265は、p_1、p_2、・・・、p_kを格納している。

離散対数計算部266は、乗算部264からg_{ab}を受け取り、

受け取ったg_{ab}について、$g \bmod p_i$に対する$g_{ab} \bmod p_i$ (i=1, 2, …, k)の離散対数$c_i \bmod p_i - 1$ (i=1, 2, …, k)を計算する。

[0091] つまり、$g_{ab} = g^{ci} \bmod p_i$ (i=1, 2, …, k)となる$c_i \bmod p_i - 1$ (i=1, 2, …, k)を求める。次に、得られた$c_i \bmod p_i - 1$ (i=1, 2, …, k)をCRT部267へ出力する。

離散対数計算部266による$ci \bmod pi-1$の計算方法については、様々なものがあるが、以下にその一例を示す。

[0092] wを1, 2, 3, …と順番に動かして、$g^w = g_{ab} \bmod p_i$となるwを求める。そのwをc_iとする。なお、各p_iに関し、g^1, g^2, …,

$g^{(pi-2)} \bmod pi$を計算した結果をテーブルとして保持し、そのテーブルの値から、$g_{ab} \bmod p_i$と一致するg^wを探す、としてもよい。

CRT部267は、離散対数計算部266から$c_i \bmod p_i - 1$ (i=1, 2, …, k)を受け取り、中国人剰余定理(CRT)により、受け取った$c_i \bmod p_i - 1$ (i=1, 2, …, k)から、$g_{ab} \bmod n$の$g \bmod n$に対する離散対数$c \bmod L$を求める。つまり、中国人剰余定理により、$c_i = c \bmod p_i - 1$ (i=1, 2, …, k)となるcを求める。

[0093] 離散対数$c_i \bmod p_i - 1$ (i＝1, 2, …, k)から、中国人剰余定理を用いて、c mod L （ここで、L＝LCM($p_1 - 1$, $p_2 - 1$, …, $p_k - 1$)）を求めるには、次に示すようにする。

ここで、式が複雑になるのを避けるために、$m_i = p_i - 1$とおく。

$u_2 = m_1 \times (m_1^{-1} \bmod (m_2/\mathrm{GCD}(m_1, m_2))) \times (c_2 - c_1) + c_1$ を計算する。

[0094] ここで、GCD(a,b,c,・・・)は、a,b,c,・・・の最大公約数(Greatest Common Divisor)を示す。

次に、

$u_3 = (m_1 \times m_2) \times ((m_1 \times m_2)^{-1} \bmod (m_3/\mathrm{GCD}(m_1, m_2, m_3))) \times (c_3 - u_2) + u_2$

を計算し、

$u_4 = (m_1 \times m_2 \times m_3) \times ((m_1 \times m_2 \times m_3)^{-1} \bmod (m_4/\mathrm{GCD}(m_1, m_2, m_3, m_4))) \times (c_4 - u_3) + u_3$ を計算し、

以下順に、同様に、$u_5, u_6, \cdots, u_{k-1}$を計算し、

$u_k = (m_1 \times m_2 \times m_3 \times \cdots \times m_{k-1}) \times ((m_1 \times m_2 \times m_3 \cdots \times m_{k-1})^{-1} \bmod (m_k/\mathrm{GCD}(m_1, m_2, m_3, m_4 \cdots, m_{k-1}))) \times (c_k - u_{k-1}) + u_{k-1}$ を計算する。

[0095] 次に、$c = u_k$とする。こうして、cが得られる。

なお、CRT部267よるc_i (i＝1, 2, . . . , k)から,

c mod $p_i - 1 = c_i$を満たすc mod Lを計算する方法については、非特許文献2に詳しく述べられている。

次に、CRT部267は、得られたcを加算モジュール243の呼び出し元のプログラムへ出力する。

[0096] (v)加算モジュール243による加算の動作

加算モジュール243による加算の動作について、図15に示すフローチャートを用いて説明する。

べき乗演算部262は、加算モジュール243の呼び出し元のプログラムから入力データa、bを受け取り(ステップS301)、受け取った入力データa、bに対し、$g_a = g^a \bmod n$, $g_b = g^b \bmod n$を計算する(ステップS302ーS303)。

[0097] 次に、乗算部264は、g_a及びg_bに対し、$g_{ab} = g_a \times g_b \bmod n$を計算する(ステッ

プS304)。

次に、離散対数計算部266は、$g_{ab} = g^{ci} \bmod p_i$ (i＝1, 2, …, k)となる$c_i \bmod p_i - 1$を求め(ステップS305)、CRT部267は、中国人剰余定理(CRT)により、$c_i = c \bmod p_i - 1$(i＝1, 2, …, k)となるcを求め(ステップS306)、次に、得られたcを加算モジュール243の呼び出し元のプログラムへ出力する(ステップS307)。

[0098] (vi)加算モジュール243による加算の動作の検証

以下で、加算モジュール243が、入力データa、bに対し、データa＋bを出力していることを検証する。

変換部251において、入力データa、bに対し、$g_a = g^a \bmod n$,
$g_b = g^b \bmod n$を計算し、主要演算部252において、
$g_{ab} = g_a \times g_b \bmod n$を計算する。このとき、$g_{ab} = g^{(a+b)} \bmod n$を満たすことは明らかである。

逆変換部253では、gとg_{ab}から$g_{ab} = g^{ci} \bmod p_i$ (i＝1, 2, …, k)を満たすc_iを計算し、その結果を用いて、$c = c_i \bmod p_i - 1$を満たす$c \bmod L$を計算する。このとき、cは$g_{ab} = g^c$
$\bmod n$を満たす。なぜなら、a＋b＝c mod Lより、$g^{(a+b-c)} = 1 \bmod n$となるためである。したがって、$g^{(a+b)} \bmod n = g^c \bmod n$を満たすため、$a + b = c \bmod ((p1-1) \times (p2-1) \times \cdots \times (pk-1))$を満たす。a＜L／2, b＜L／2よりa＋b＜Lであるので、加算モジュール243は、入力データaと入力データbとの加算結果であるデータa＋bを出力していることになる。

[0099] 1．4 第1の実施の形態の効果

加算モジュール243は、加算を行う値を変換している。変換部251及び逆変換部253が解析困難な場合であっても、解析者はg_a, g_b, g_{ab}の値を知り、g_a, g_bからg_{ab}を計算する処理を知る可能性がある。このような場合であっても、変換後の値g_a, g_bから変換前の値a, bを推測することは困難である。さらに、加算モジュール243は、主要演算部252において、乗算を行っており、この乗算という演算から加算モジュール243が加算を実現していることを推測することは困難である。したがって、加算を行う入力の値の隠蔽だけではなく、加算という演算自体も隠蔽できることになり、第1の実

施の形態は有効である。

[0100] 復号制御モジュール241は、鍵と他のデータとの加算において、加算モジュール243を利用している。そのため、加算の対象となる値、すわなち、鍵の値を推測することが困難になる。また、解析者が暗号アルゴリズムを知っている場合においても、鍵加算部分が、鍵との「加算」を行っていると推測しにくい。そのため、解析者が、暗号アルゴリズムの特徴である鍵加算部分をプログラム内から探し出す攻撃をした場合でも、鍵加算部分を探し出すことが困難なため、攻撃も困難となる。このように、解析者の攻撃が困難になり、本実施の形態は有効である。

[0101] 2. 変形例(1)

第1の実施の形態における加算モジュール243の代わりに、加算モジュール501を採用するとしてもよい。ここでは、加算モジュール501について説明する。

2. 1 加算モジュール501の構成

加算モジュール501は、加算モジュール243と同様に、入力データa、bに対し、データa+bを演算し、データa+bを出力するコンピュータプログラムであり、図16に示すように、変換部511、主要演算部512及び逆変換部513から構成されており、変換部511は、パラメタ格納部521、乱数発生部522及びべき乗演算部523を含み、主要演算部512は、パラメタ格納部524及び乗算部525を含み、逆変換部513は、パラメタ格納部526、離散対数計算部527及び還元部528を含む。

[0102] 2. 2 各種パラメータ及び記号の定義、並びに入力データの条件

ここで、加算モジュール501で使用する各種パラメータ及び記号の定義、並びに入力データの条件について説明する。

p, qを素数とし、$n=p^2 \times q$とする。p, qは、逆変換部513により保持され、nは、それぞれ、変換部511及び主要演算部512により保持される。

[0103] 加算モジュール501では、mod nの整数から構成される剰余整数環Z/nZの乗法群の演算を用いる。gは、その乗法群に属する予め与えられた数であり$g^{(p-1)} \mod p^2$の位数がpである数とする。また、

$g_p = g^{(p-1)} \mod p^2$と定義する。

入力データa、bは、p/2より小さい非負整数とする。

[0104] 2．3 変換部511の構成

変換部511は、パラメタ格納部521、乱数発生部522及びべき乗演算部523から構成されている。

パラメタ格納部521は、nとgとを記憶している。

乱数発生部522は、n以下の乱数R1，R2を生成する。

[0105] べき乗演算部523は、入力データa、bに対し、乱数発生部522により生成された乱数R1，R2を用いて、

$g_a = g\hat{}(a+n\times R1) \mod n$、

$g_b = g\hat{}(b+n\times R2) \mod n$を計算する。

なお、本明細書において、記号「^」は、べき乗を示す演算子である。例えば、a^b＝a^bである。本明細書において、表現上の都合により、a^b及びa^bの両方の表記を使い分けている。

[0106] 次に、べき乗演算部523は、計算結果g_a，g_bを主要演算部512へ出力する。

2．4 主要演算部512の構成

主要演算部512は、パラメタ格納部524及び乗算部525から構成されている。

パラメタ格納部524は、nを記憶している。

乗算部525は、べき乗演算部523から計算結果g_a，g_bを受け取り、受け取ったg_a，g_bに対し、

$g_{ab} = g_a \times g_b \mod n$を計算し、計算結果$g_{ab}$を逆変換部513へ出力する。

[0107] 2．5 逆変換部513の構成

逆変換部513は、パラメタ格納部526、離散対数計算部527及び還元部528から構成されている。

パラメタ格納部526は、pを格納している。

離散対数計算部527は、乗算部525から計算結果g_{ab}を受け取り、受け取ったg_{ab}に対し、パラメタ格納部526に格納されているpを用いて、

$c_p = g_{ab}^{(p-1)} \mod p^2$を計算し、次に、$c_p$を還元部528へ出力する。

[0108] 還元部528は、離散対数計算部527からc_pを受け取り、

受け取ったc_pを用いて、mod p^2におけるg_pに対するc_pの離散対数cを計算し、計

算して得られたcを、呼び出し元のプログラムへ出力する。

還元部528におけるcの計算方法については、特許文献2に詳しく述べられている。具体的には、以下のように行う。

[0109] c_p に対し、$c=(c_p-1)/(g_p-1) \mod p$としてcを求める。

2．6 加算モジュール501による加算の動作

加算モジュール501による加算の動作について、図17に示すフローチャートを用いて説明する。

べき乗演算部523は、呼び出し元のプログラムから入力データa、bを受け取り(ステップS311)、乱数発生部522は、n以下の乱数R1，R2を生成し(ステップS312)、べき乗演算部523は、

$g_a=g\hat{}(a+n\times R1) \mod n$、

$g_b=g\hat{}(b+n\times R2) \mod n$を計算する(ステップS313ーS314)。

[0110] なお、本明細書において、記号「^」は、べき乗を示す演算子であり、例えば、a^b＝a^bである。本明細書では、場合によって、「a^b」及び「a^b」の両方の表記を使い分けている。

次に、乗算部525は、$g_{ab}=g_a\times g_b \mod n$を計算する(ステップS315)。

[0111] 次に、離散対数計算部527は、$c_p=g_{ab}^{(p-1)} \mod p^2$を計算し(ステップS316)、還元部528は、$c=(c_p-1)/(g_p-1) \mod p$としてcを求め(ステップS317)、次に、c(＝a＋b)を呼び出し元のプログラムへ出力する(ステップS318)。

[0112] 2．7 加算モジュール501による加算の動作の検証

以下において、加算モジュール501が、入力データa、bに対し、a＋bを出力していることを検証する。

変換部511において、a，bに対し、

$g_a=g\hat{}(a+n\times R1) \mod n$、

$g_b=g\hat{}(b+n\times R2) \mod n$を計算し、

主要演算部512において、$g_{ab}=g_a\times g_b \mod n$を計算する。このとき、$g_{ab}=g\hat{}(a+b+n\times(R1+R2)) \mod n$を満たすことは明らかである。逆変換部513では、まず、

$c_p = g_{ab}^{(p-1)} = g_p \hat{}\ (a+b+n\times(R1+R2)) \bmod p^2$ となり、

$g_p^{p} = 1 \bmod p^2$ より、

$g_p^{n} = 1 \bmod p^2$ であるため、

$c_p = g_p^{(a+b)} \bmod p^2$ となる。

[0113] 逆変換部513では、さらに、$\bmod p^2$ におけるg_p に対するc_p の離散対数cを求める。すなわち、

$c_p = g_p^{c} \bmod p^2$ が成り立つ。したがって、

$c = a+b \bmod p$であり、$a < p/2$, $b < p/2$より、$a+b < p$であるため、加算モジュール501は、入力データaとbの加算結果a＋bを出力していることになる。

[0114] 2．8 加算モジュール501による効果

加算モジュール501は、第1の実施の形態1の加算モジュール243と同様に、加算を行う値を変換しており、変換部511及び逆変換部513が解析困難な場合に、変換後の値から変換前の値を推測することは困難である。さらに、加算モジュール501は、主要演算部512において、乗算を行っており、この乗算という演算から加算モジュール501が加算を実現していることを推測することは困難である。したがって、加算を行う入力の値の隠蔽だけではなく、加算という演算自体も隠蔽できることになり、この発明は有効である。

[0115] 2．9 その他(1)

加算モジュール501では、剰余整数環Z／nZの乗法群における冪乗演算を変換部511で行い、その乗法群の部分群である剰余整数環Z／p^2 Zの乗法群における離散対数問題を逆変換部513で解いている。ここで、もし、解析者がp，qは分からないが、変換部511で冪乗演算を行っていることを解析できた場合を考える。このケースは、すなわち、逆変換部513のみが解析者により解析困難である場合である。この場合においても、nの大きさが素因数分解が困難なぐらい、例えば、1024ビットぐらいであれば、nの素因数分解結果であるp，qを得ることが困難になる。また、p，qが得られなければ、剰余整数環Z／nZの乗法群における離散対数問題を解くことが困難になる。一般に乗法群の大きさ(元の数)が1024ビットの数のように大きい場合は、それ上の離散対数問題も困難になる。加算モジュール501では、pが既知の場合は逆変

換部513における逆変換の方法によって、Z／p^2 Zの乗法群における離散対数問題を容易に解けるようになる。加算モジュール501における変換はこのように、pが既知であれば逆変換が容易であるが、既知でなければ困難であることを利用している点が、加算モジュール2431と異なる。

[0116] 2．10 その他(2)

加算モジュール501は、次のように構成してもよい。

p，qを素数とし、n＝p^m ×qとする。mは、正整数である。また、加算モジュール501では、mod nの整数から構成される剰余整数環Z／nZの乗法群の演算を用いる。gは、その乗法群に属する予め与えられた数であり$g^{(p-1)}$ mod p^m の位数がpである数とする。また、g_p ＝$g^{(p-1)}$ mod p^m と定義する。

[0117] 離散対数計算部527は、乗算部525から計算結果g_{ab}を受け取り、受け取ったg_{ab}に対し、パラメタ格納部526に格納されているpを用いて、

c_p ＝$g_{ab}^{(p-1)}$ mod p^m を計算し、次に、c_p を還元部528へ出力する。

還元部528は、離散対数計算部527からc_p を受け取り、

受け取ったc_p を用いて、mod p^m におけるg_p に対するc_p の離散対数cを計算し、計算して得られたcを、呼び出し元のプログラムへ出力する。

[0118] 3．変形例(2)

第1の実施の形態における加算モジュール243の代わりに、加算モジュール601を採用するとしてもよい。ここでは、加算モジュール601について説明する。加算モジュール601は、楕円曲線上のスカラ倍演算を利用している。楕円曲線については、非特許文献3に詳しく説明されている。

[0119] 3．1 加算モジュール601の構成

加算モジュール601は、加算モジュール243と同様に、入力データa、bに対し、データa＋bを演算し、データa＋bを出力するコンピュータプログラムであり、図18に示すように、変換部611、主要演算部612及び逆変換部613から構成されており、変換部611は、パラメタ格納部621及びスカラ倍演算部622を含み、主要演算部612は、パラメタ格納部623及び楕円曲線加算部624を含み、逆変換部613は、パラメタ格納部625、還元部626及び離散対数計算部627を含む。

[0120] 3．2 各種パラメータ及び記号の定義、並びに入力データの条件

ここで、加算モジュール601で使用する各種パラメータ及び記号の定義、並びに入力データの条件について説明する。

p、qを素数とし、n＝p×qとする。p、qは、逆変換部613により保持され、nは、それぞれ、変換部611及び主要演算部612により保持されている。

[0121] 楕円曲線Eの方程式を

$y^2 = x^3 + A \times x + B$とする。ここで、A、Bは、楕円曲線Eのパラメータである。

$G = (x_g, y_g) \mod n$を楕円曲線E上の点とする。すなわち、

$y_g^2 = x_g^3 + A \times x_g + B \mod n$を満たす。

A、B、Gは、変換部611、主要演算部612、逆変換部613により保持される。

[0122] 楕円曲線Eの方程式をもつ体GF(p)上の楕円曲線の点から構成される群をE(GF(p))と表現する。同様に、楕円曲線Eの方程式をもつ体GF(q)上の楕円曲線の点から構成される群をE(GF(q))と表現する。

Z／nZ上の楕円曲線の群を

E(GF(p))とE(GF(q))との

直積E(GF(p))×E(GF(q))で表す。なお、Z／nZは体ではなく、環であるため、数学的には楕円曲線とは呼べないが、ここでは便宜上、その直積Z／nZ上の楕円曲線の群とよぶ。

[0123] E(GF(p))上の点$G_p = (x_{gp}, y_{gp}) \mod p$と、

E(GF(q))上の点$G_q = (x_{gq}, y_{gq}) \mod q$とに対応するZ／nZ上の楕円曲線E(GF(p))×E(GF(q))の

点$G = (x_g, y_g) \mod n$について、

x_gを

$x_g \mod p = x_{gp}$及び

$x_g \mod q = x_{gq}$を満たす数と定義し、

y_gを

$y_g \mod p = y_{gp}$及び

$x_g \mod q = x_{gq}$を満たす数と定義する。

[0124] この定義より、

E(GF(p))×E(GF(q))上の点G＝(x_g, y_g) mod nに対応するE(GF(p))上の点G_pを

G_p＝(x_{gp}, y_{gp}) mod pとし、

E(GF(q))上の点G_qをG_q＝(x_{gq}, y_{gq})とすることで、

E(GF(p)), E(GF(q))をE(GF(p))×E(GF(q))の部分群とみなす。

[0125] 加算部601においては、上記楕円曲線Eは、mod pでの楕円曲線の位数、すなわち、点の個数が、pであるとする。このような体GF(p)上の楕円曲線をアノマラス(Anomalous)楕円曲線とよぶ。

さらに、mod qでの楕円曲線の位数がqである、すなわち、GF(q)上でもアノマラス楕円曲線であるとする。

[0126] このとき、Z／nZ上の楕円曲線を、スーパーアノマラス(Super-Anomalous)楕円曲線とよぶ。スーパーアノマラス楕円曲線については非特許文献4に詳しく説明されている。

このとき、Z／nZ上の楕円曲線の群はE(GF(p))×E(GF(q))であるので、楕円曲線の位数は、

n(＝p×q)となる。

[0127] 入力データa、bは、p／2より小さい非負整数とする。

3．3 変換部611の構成

変換部611は、パラメタ格納部621及びスカラ倍演算部622から構成されている。

パラメタ格納部621は、n、A、B、Gを記憶している。

[0128] スカラ倍演算部622は、呼び出し元のプログラムから、入力データa、bを受け取り、受け取った入力データa、bに対し、パラメータ格納部621に格納されているn、A、B、Gを用いて、

G_a＝a＊G mod n 及び

G_b＝b＊G mod nを計算する。

[0129] ここで、a＊Gは、Gをa回、楕円曲線の加算により足し合わせて得られる点である。また、a＊G mod nは、a＊Gの各座標に、mod nを施したものである。

スカラ倍演算部622は、計算結果G_a，G_bを主要演算部612へ出力する。

3．4　主要演算部612の構成

主要演算部612は、パラメタ格納部623及び楕円曲線加算部624から構成されている。

[0130]　パラメタ格納部623は、n、A、Bを記憶している。

楕円曲線加算部624は、スカラ倍演算部622から計算結果G_a，G_bを受け取り、パラメタ格納部623に記憶されているn、A、Bを用いて、G_a及びG_bに対して、楕円曲線加算を実行して、

$$G_{ab} = G_a + G_b \mod n$$

を計算し、その計算結果G_{ab}を逆変換部613へ出力する。

[0131]　3．5　逆変換部613の構成

逆変換部613は、パラメタ格納部625、還元部626及び離散対数計算部627から構成されている。

パラメタ格納部625は、p，A，B，G mod pを記憶している。

還元部626は、楕円曲線加算部624から計算結果G_{ab}を受け取り、受け取ったG_{ab}に対し、パラメタ格納部625に格納されているpを用いて、

$G_{abp} = G_{ab} \mod p$ を計算し、計算結果を離散対数計算部627へ出力する。

[0132]　離散対数計算部627は、G mod pに対するG_{abp}の離散対数c mod pを計算する。つまり、$G_{abp} = c * G \mod p$のcを求める。次に、cを呼び出し元のプログラムへ出力する。

ここで、楕円離散対数計算部627におけるcは、アノマラス楕円曲線上の離散対数問題の解である。アノマラス楕円曲線上の離散対数問題を解く方法については、非特許文献3の88ー91ページに詳しく説明されている。計算方法はこの文献に記載されているため、ここでは説明を省略する。

[0133]　3．6　加算モジュール601の動作

加算モジュール601の動作について、図19に示すフローチャートを用いて説明する。

スカラ倍演算部622は、呼び出し元のプログラムから、入力データa、bを受け取り（

ステップS321)、受け取った入力データa、bに対し、パラメータ格納部621に格納されているn、A、B、Gを用いて、

G_a ＝a＊G mod n 及び

G_b ＝b＊G mod nを計算する(ステップS322ーS323)。

[0134] 次に、楕円曲線加算部624は、

G_{ab} ＝G_a ＋G_b mod nを計算する(ステップS324)。

次に、還元部626は、

G_{abp} ＝G_{ab} mod p を計算し(ステップS325)、

離散対数計算部627は、G mod pに対するG_{abp}の離散対数cを計算し(ステップS326)、次に、cを呼び出し元のプログラムへ出力する(ステップS327)。

[0135] 3．7 加算モジュール601の動作検証

以下において、加算モジュール601が、入力データa，bに対し、a＋bを計算して出力していることを検証する。

変換部611において、a，bに対し、

G_a ＝a＊G mod n,

G_b ＝b＊G mod nを計算し、

主要演算部612において、

Gab＝Ga＋Gb mod nを計算する。

[0136] このとき、Gab＝(a＋b)＊G mod nを満たすことは明らかである。

逆変換部613において、まず、

G_{abp} ＝Gab mod pを計算し、

G mod pに対するG_{abp}の離散対数cを求める。

すなわち、G_{abp} ＝c＊G mod pが成り立つ。

[0137] 従って、c＝a＋b mod pであり、a＜p／2，b＜p／2より、

a＋b＜pであるため、加算モジュール601は、入力データaとbとの加算結果a＋bを出力していることになる。

3．8 加算モジュール601の効果

加算モジュール601は、加算モジュール243及び、加算モジュール501と同様に、

加算を行う値を変換しており、変換部611及び逆変換部613が解析困難な場合に、変換後の値から変換前の値を推測することは困難である。

[0138] さらに、加算モジュール601は、主要演算部612において、楕円曲線加算を行っており、この楕円曲線加算という演算から加算モジュール601が整数の加算を実現していることを推測することは困難である。

従って、整数の加算を行う入力の値の隠蔽だけではなく、整数の加算という演算自体も隠蔽できることになり、加算モジュール601は、有効である。

[0139] 3．9 その他

加算モジュール601では、Z／nZ上の楕円曲線の群E(GF(p))×E(GF(q))のスカラ倍演算を変換部で行い、その部分群であるE(GF(p))における離散対数問題を逆変換部で解いている。

ここで、もし、解析者がp，qは分からないが、変換部で冪乗演算を行っていることを解析できた場合を考える。このケースは、すなわち、逆変換部のみが解析者により解析困難である場合である。

[0140] この場合においても、nの大きさが素因数分解が困難なぐらい、例えば、1024ビットぐらいであれば、nの素因数分解結果であるp，qを得ることが困難になる。また、p，qが得られなければ、Z／nZ上の楕円曲線の群E(GF(p))×E(GF(q))における離散対数問題を解くことが困難になる。

一般に群の大きさ(元の数)が1024ビットの数のように大きい場合は、それ上の離散対数問題も困難になる。加算モジュール601では、pが既知の場合は逆変換モジュールにおける逆変換の方法によって、楕円曲線の群E(GF(p))における離散対数問題を容易に解けるようになる。加算モジュール601における変換はこのように、pが既知であれば逆変換が容易であるが、既知でなければ困難であることを利用している点が、第1の実施の形態と異なる。

[0141] 4．その他の変形例

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

（1）加算モジュール243、501及び601において、2個の非負整数a及びbの加算を行うとしているが、各加算モジュールは、3個、又はそれ以上の個数の非負整数の加算を行うとしてもよい。この場合に、各加算モジュールの変換部は、それぞれの非負整数を変換し、加算モジュール243及び501の主要演算部は、それぞれの変換結果に対して乗算を施し、加算モジュール601の主要演算部は、それぞれの変換結果に対して、楕円曲線加算を施す。

[0142] （2）復号制御モジュール241において、鍵加算部分のみに加算モジュール243、501又は601を使用するとしているが、他の加算部分において、各加算モジュールを使用するとしてもよい。

（3）第1の実施の形態では、各加算モジュールを復号制御モジュール241に適用するとしているが、上記の暗号制御モジュール141や、他の暗号プログラム、復号プログラム、デジタル署名を生成する署名生成プログラムに適用するとしてもよい。このように、加算による演算が出現する情報処理演算であれば、どのようなものであっても適用することができる。

[0143] （4）加算モジュール243、501及び601において、剰余整数環の乗法群、楕円曲線上の群を利用したが、その他の群を利用するとしてもよい。

また、加算モジュール243及び501においては、冪乗演算を行って、整数を変換し、加算モジュール601においては、楕円曲線のスカラ倍演算を行って、整数を変換するとしているが、その他の群の冪演算を行うことにより変換するとしてもよい。

[0144] ここで、冪演算とは、群の基本演算、すなわち、剰余整数環では乗算を、また楕円曲線上の群では楕円曲線加算を、整数回行った結果を求める演算である。

したがって、剰余整数環の乗法群の冪演算は冪乗演算、楕円曲線上の群の冪演算は楕円曲線のスカラ倍演算である。

加算モジュール501では、剰余整数環Z／nZの乗法群の「部分群」である、剰余整数環Z／p^2 Zの乗法群において離散対数問題を解いている。その他の群を使用する場合は、加算モジュール501と同様に逆変換部でその他の群の「部分群」において離散対数問題を解くとしてもよい。

[0145] （5）加算モジュール243において、gは、mod p_i （i＝1，2，…，k）において原始

元としたが、原始元でなくてもよい。

その場合は、$g^{mi} = 1 \mod p_i$ ($m_i > 0$)となるm_iに対し、

$L = m_1 \times m_2 \times \cdots \times m_k$とする。

(6)上記の各装置は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレィユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。ここで、コンピュータプログラムは、所定の機能を達成するために、コンピュータに対する指令を示す命令コードが複数個組み合わされて構成されたものである。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、各装置は、その機能を達成する。つまり、前記マイクロプロセッサは、前記コンピュータプログラムに含まれる各命令を1個ずつ読み出し、読み出した命令を解読し、解読結果に従って動作する。

[0146] (7)上記の各装置を構成する構成要素の一部又は全部は、1個のシステムLSI(Large Scale Integration:大規模集積回路)から構成されているとしてもよい。システムLSIは、複数の構成部を1個のチップ上に集積して製造された超多機能LSIであり、具体的には、マイクロプロセッサ、ROM、RAMなどを含んで構成されるコンピュータシステムである。前記RAMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、システムLSIは、その機能を達成する。

[0147] (8)上記の各装置を構成する構成要素の一部又は全部は、各装置に脱着可能なICカード又は単体のモジュールから構成されているとしてもよい。前記ICカード又は前記モジュールは、マイクロプロセッサ、ROM、RAM、などから構成されるコンピュータシステムである。前記ICカード又は前記モジュールは、上記の超多機能LSIを含むとしてもよい。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、前記ICカード又は前記モジュールは、その機能を達成する。このICカード又はこのモジュールは、耐タンパ性を有するとしてもよい。

[0148] (9)本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプ

ログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD−ROM、MO、DVD、DVD−ROM、DVD−RAM、BD（Blu−ray Disc）、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

[0149] また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

[0150] また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

（10）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

（11）以上説明したように、本発明によると、演算に使用する値の隠蔽だけでなく、演算そのものを隠蔽することができる。したがって、本技術を用いた難読化ソフトウェアをICカード等の機器に組み込むことは有用である。

産業上の利用可能性

[0151] 本発明を構成する各装置、各方法及び各コンピュータプログラムは、情報を安全かつ確実に扱う必要があるあらゆる産業において、経営的に、また継続的及び反復的に使用することができる。また、本発明を構成する各装置、各方法及び各コンピュータプログラムは、電器機器製造産業において、経営的に、また継続的及び反復的に、製造し、販売することができる。

請求の範囲

[1] 2個以上の整数を加算するコンピュータシステムであって、

複数のコンピュータ命令が組み合わされて構成されるコンピュータプログラムを記憶しているメモリ部と、

前記記憶手段に記憶されている前記コンピュータプログラムから1個ずつコンピュータ命令を読み出し、解読し、その解読結果に応じて動作するプロセッサとを備え、

前記コンピュータプログラムは、

各整数に、群G上の冪演算を施すことにより、群Gに属する元を生成する変換命令群と、

生成された全ての前記元に対して、前記加算とは異なる群G上の基本演算を施して、演算値を生成する演算命令群と、

群G又は群Gに真に含まれる部分群Sにおいて、前記演算値に対して、前記変換命令群により施される冪演算の逆算を施すことにより、前記整数の加算値を生成する逆変換命令群とを含む

ことを特徴とするコンピュータシステム。

[2] 前記コンピュータシステムは、対象情報を安全かつ確実に扱う情報セキュリティ装置であって、

前記コンピュータプログラムは、さらに、対象情報にセキュリティ処理を施すセキュリティ命令群を含み、

前記セキュリティ命令群は、加算演算において、前記変換命令群、前記演算命令群及び前記逆変換命令群を用いる

ことを特徴とする請求項1に記載のコンピュータシステム。

[3] 前記群Gは、剰余整数環の乗法群であり、

前記変換命令群は、各整数に冪乗を施し、

演算命令群は、前記元に対して、乗算を施す

ことを特徴とする請求項2に記載のコンピュータシステム。

[4] 前記群Gは、複数個の相異なる素数p_1，p_2，…，p_k（k＞1）の積n＝p_1×p_2×…×p_kに対し、Z／nZの乗法群であり、

×は、乗算を示す演算子であり、Zは、整数環であり、Z／nZは、mを法とし整数と合同である値から構成される剰余整数環である

ことを特徴とする請求項3に記載のコンピュータシステム。

[5] 前記逆変換命令群は、前記素数p_1，p_2，…，p_kを用いたZ／p_1 Z、Z／p_2 Z、…、Z／p_k Zの乗法群における離散対数問題を解く命令を含む

ことを特徴とする請求項4に記載のコンピュータシステム。

[6] 前記逆変換命令群は、前記素数p_1，p_2，…，p_kを用いたZ／p_1 Z，Z／p_2 Z，…，Z／p_k Zの乗法群における離散対数問題の解に対し、中国人の剰余定理を用いる命令を含む

ことを特徴とする請求項5に記載のコンピュータシステム。

[7] 前記群Gは、2つの素数p，qと正整数mを用いて表されるn＝p^m ×qに対し、Z／nZの乗法群であり、

前記変換命令群は、各整数に冪乗を施し、

演算命令群は、前記元に対して、乗算を施す

ことを特徴とする請求項2に記載のコンピュータシステム。

[8] 前記部分群Sは、Z／p^m Zの乗法群である

ことを特徴とする請求項7に記載のコンピュータシステム。

[9] 前記正整数mは、2である

ことを特徴とする請求項7に記載のコンピュータシステム。

[10] 前記部分群Sは、アノマラス楕円曲線の群であり、

前記変換命令群は、各整数に楕円曲線上の乗算を施し、

演算命令群は、前記元に対して、楕円曲線上の加算を施す

ことを特徴とする請求項2に記載のコンピュータシステム。

[11] 前記群Gは、二つのアノマラス楕円曲線の群の直積であり、

前記変換命令群は、各整数に楕円曲線上の乗算を施し、

演算命令群は、前記元に対して、楕円曲線上の加算を施す

ことを特徴とする請求項2に記載のコンピュータシステム。

[12] さらに、前記逆変換命令群は、複数の冪数と、各冪数による冪乗値又は冪倍値とを

対応付けて記憶しており、その対応付けを検索することにより、冪演算の逆算を求める

ことを特徴とする請求項2に記載のコンピュータシステム。

[13] さらに、前記逆変換命令群は、前記群Gに属する元を前記部分群Sに属する元に還元する還元部を備える

ことを特徴とする請求項2に記載のコンピュータシステム。

[14] 前記情報セキュリティ装置は、鍵情報に基づいて対象情報を暗号化し又は復号し、

前記セキュリティ命令群は、前記鍵情報に基づいて、対象情報を暗号化し又は復号し、暗号化又は復号において、鍵情報又は鍵情報から得られる二次鍵情報と、対象情報又は対象情報から得られる二次対象情報との加算演算が含まれ、

前記加算演算において、前記変換命令群、前記演算命令群及び前記逆変換命令群を用いて、鍵情報又は鍵情報から得られる二次鍵情報と、対象情報又は対象情報から得られる二次対象情報とに、加算を施す

ことを特徴とする請求項2に記載のコンピュータシステム。

[15] 前記暗号化又は復号は、共通鍵方式の暗号化又は復号アルゴリズムである

ことを特徴とする請求項14に記載のコンピュータシステム。

[16] 前記情報セキュリティ装置は、鍵情報に基づいて対象情報にデジタル署名を施し又は署名検証を施し、

前記セキュリティ命令群は、前記鍵情報に基づいて、対象情報にデジタル署名を施し又は署名検証を施し、デジタル署名又は署名検証において、鍵情報又は鍵情報から得られる二次鍵情報と、対象情報又は対象情報から得られる二次対象情報との加算演算が含まれ、

前記加算演算において、前記変換命令群、前記演算命令群及び前記逆変換命令群を用いて、鍵情報又は鍵情報から得られる二次鍵情報と、対象情報又は対象情報から得られる二次対象情報とに、加算を施す

ことを特徴とする請求項2に記載のコンピュータシステム。

[17] 前記コンピュータシステムは、前記メモリ部と前記プロセッサとが高密度に集積された集積回路を含むICカードである

ことを特徴とする請求項2に記載のコンピュータシステム。

[18] メモリ部とプロセッサとを備えるコンピュータシステムにおいて用いられ、2個以上の整数を加算する加算方法であって、

各整数に、群G上の冪演算を施すことにより、群Gに属する元を生成する変換ステップと、

生成された全ての前記元に対して、前記加算とは異なる群G上の基本演算を施して、演算値を生成する演算ステップと、

群G又は群Gに真に含まれる部分群Sにおいて、前記演算値に対して、前記変換命令群により施される冪演算の逆算を施すことにより、前記整数の加算値を生成する逆変換ステップとを含む

ことを特徴とする加算方法。

[19] 2個以上の整数を加算するコンピュータプログラムであって、

各整数に、群G上の冪演算を施すことにより、群Gに属する元を生成する変換命令群と、

生成された全ての前記元に対して、前記加算とは異なる群G上の基本演算を施して、演算値を生成する演算命令群と、

群G又は群Gに真に含まれる部分群Sにおいて、前記演算値に対して、前記変換命令群により施される冪演算の逆算を施すことにより、前記整数の加算値を生成する逆変換命令群とを含む

ことを特徴とするコンピュータプログラム。

[20] 前記コンピュータプログラムは、コンピュータ読み取り可能な記録媒体に記録されている

ことを特徴とする請求項19に記載のコンピュータプログラム。

[21] 前記コンピュータプログラムは、搬送波に乗せられて送信される

ことを特徴とする請求項19に記載のコンピュータプログラム。

[22] 2個以上の整数を加算するコンピュータプログラムを記録しているコンピュータ読み取り可能な記録媒体であって、

前記コンピュータプログラムは、

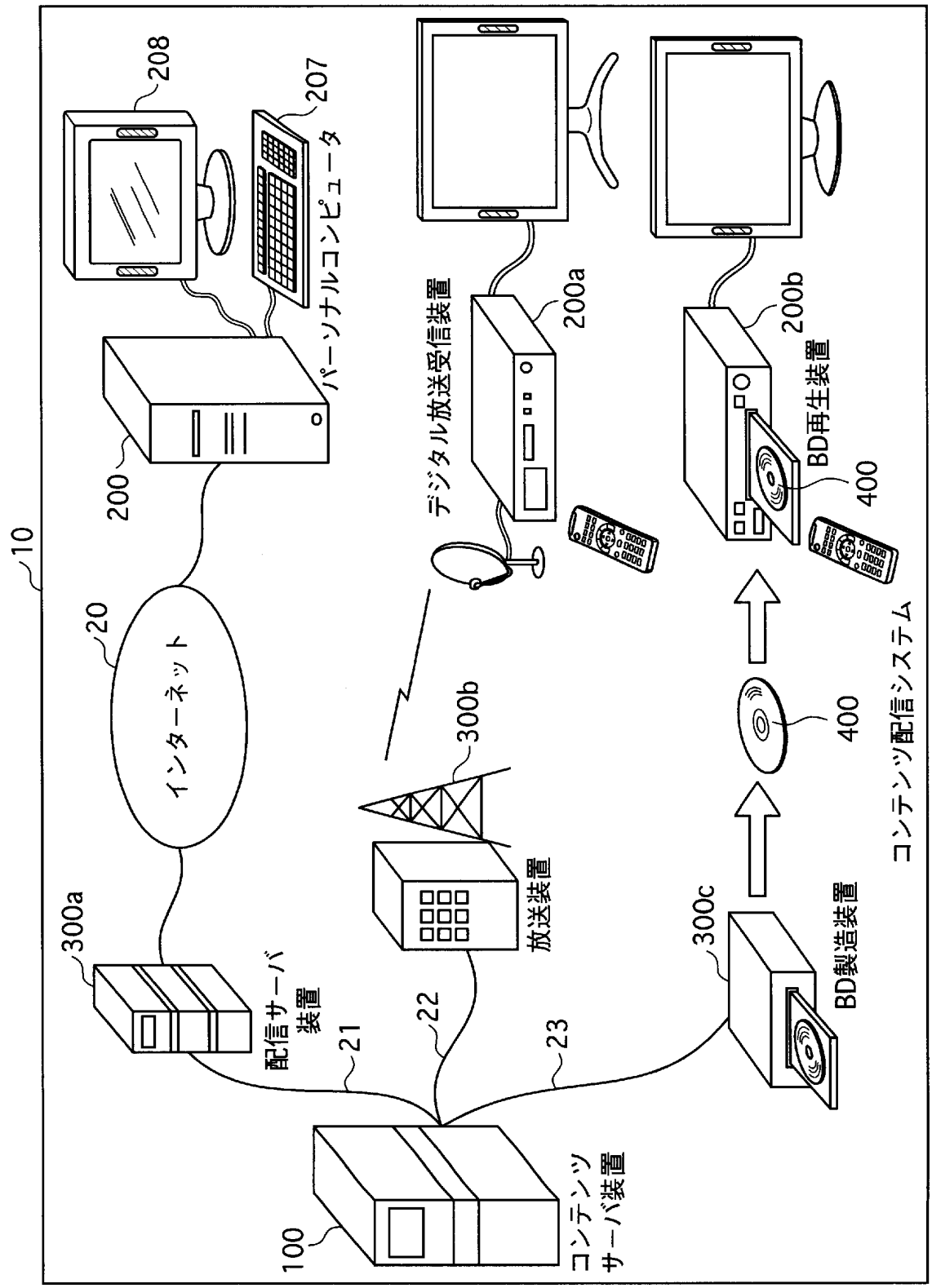
各整数に、群G上の冪演算を施すことにより、群Gに属する元を生成する変換命令群と、

生成された全ての前記元に対して、前記加算とは異なる群G上の基本演算を施して、演算値を生成する演算命令群と、

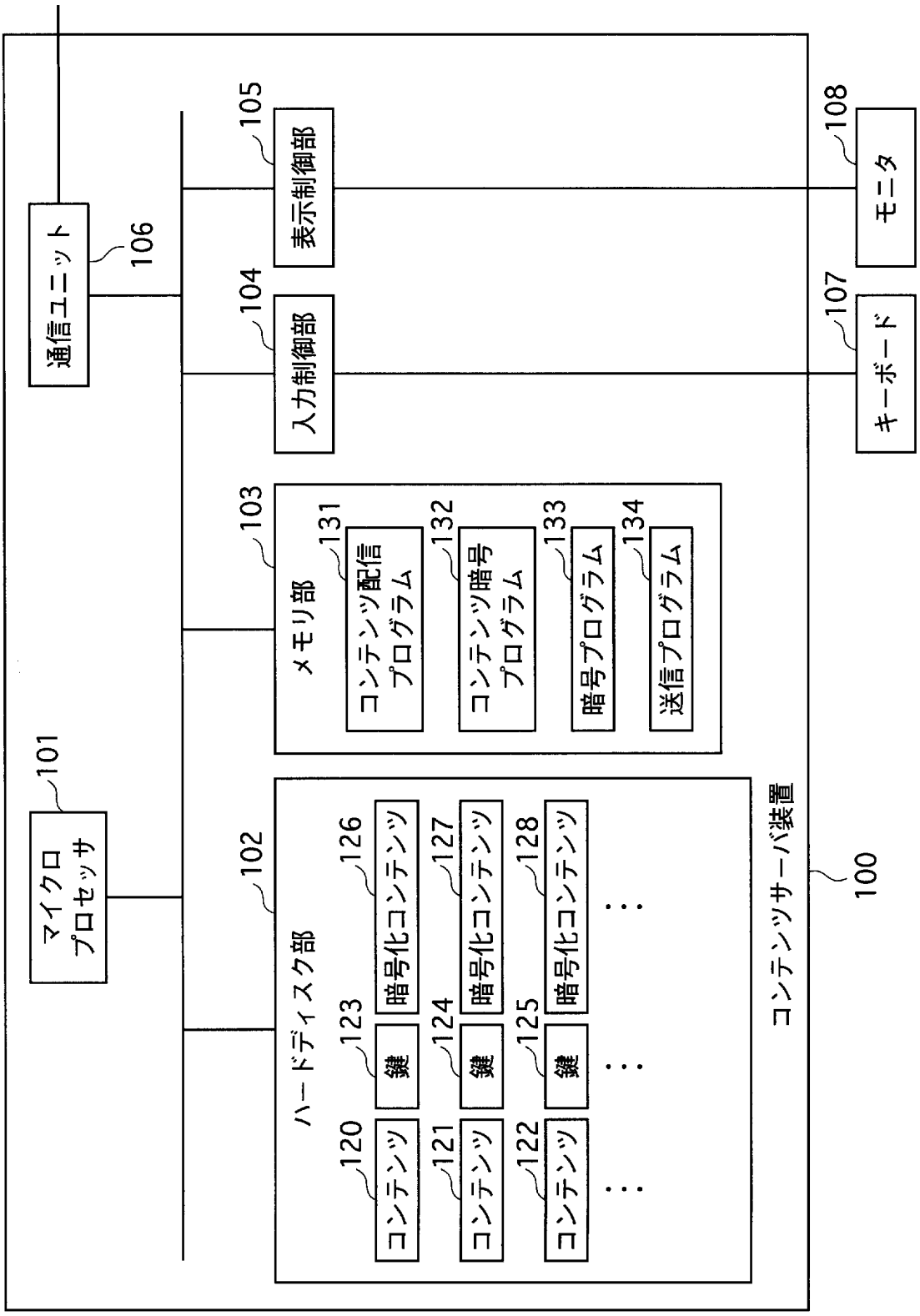
群G又は群Gに真に含まれる部分群Sにおいて、前記演算値に対して、前記変換命令群により施される冪演算の逆算を施すことにより、前記整数の加算値を生成する逆変換命令群とを含む

ことを特徴とする記録媒体。

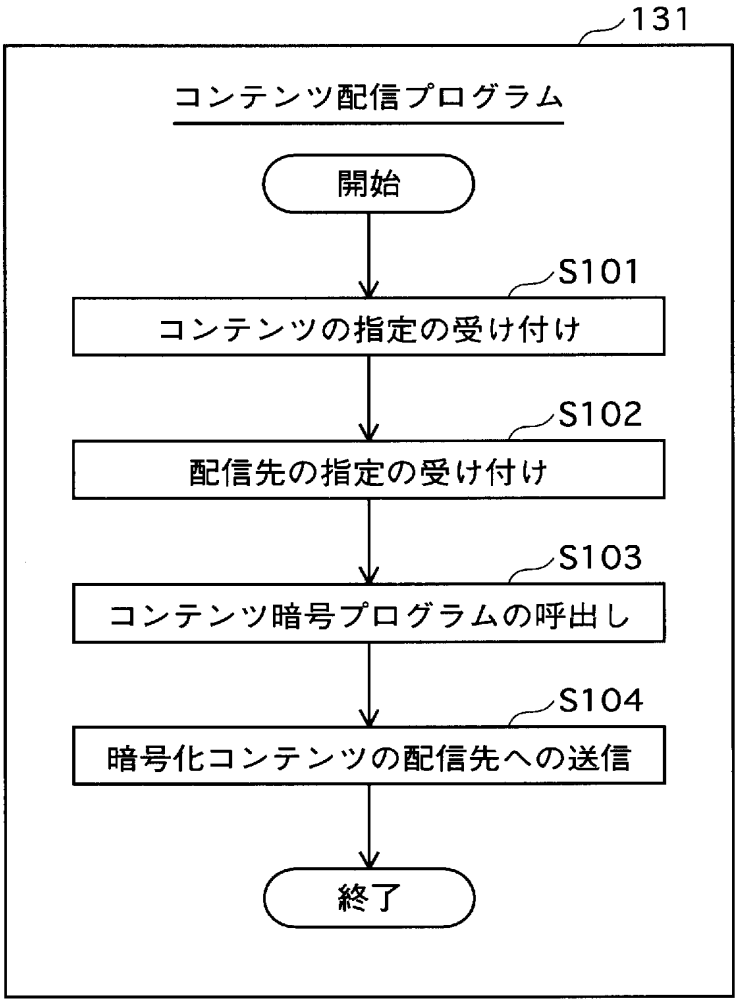
[図1]


10
208
207
パーソナルコンピュータ
200
20
インターネット
デジタル放送受信装置
200a
200b
BD再生装置
400
300a
配信サーバ装置
21
300b
放送装置
22
23
300c
BD製造装置
400
100
コンテンツサーバ装置
コンテンツ配信システム

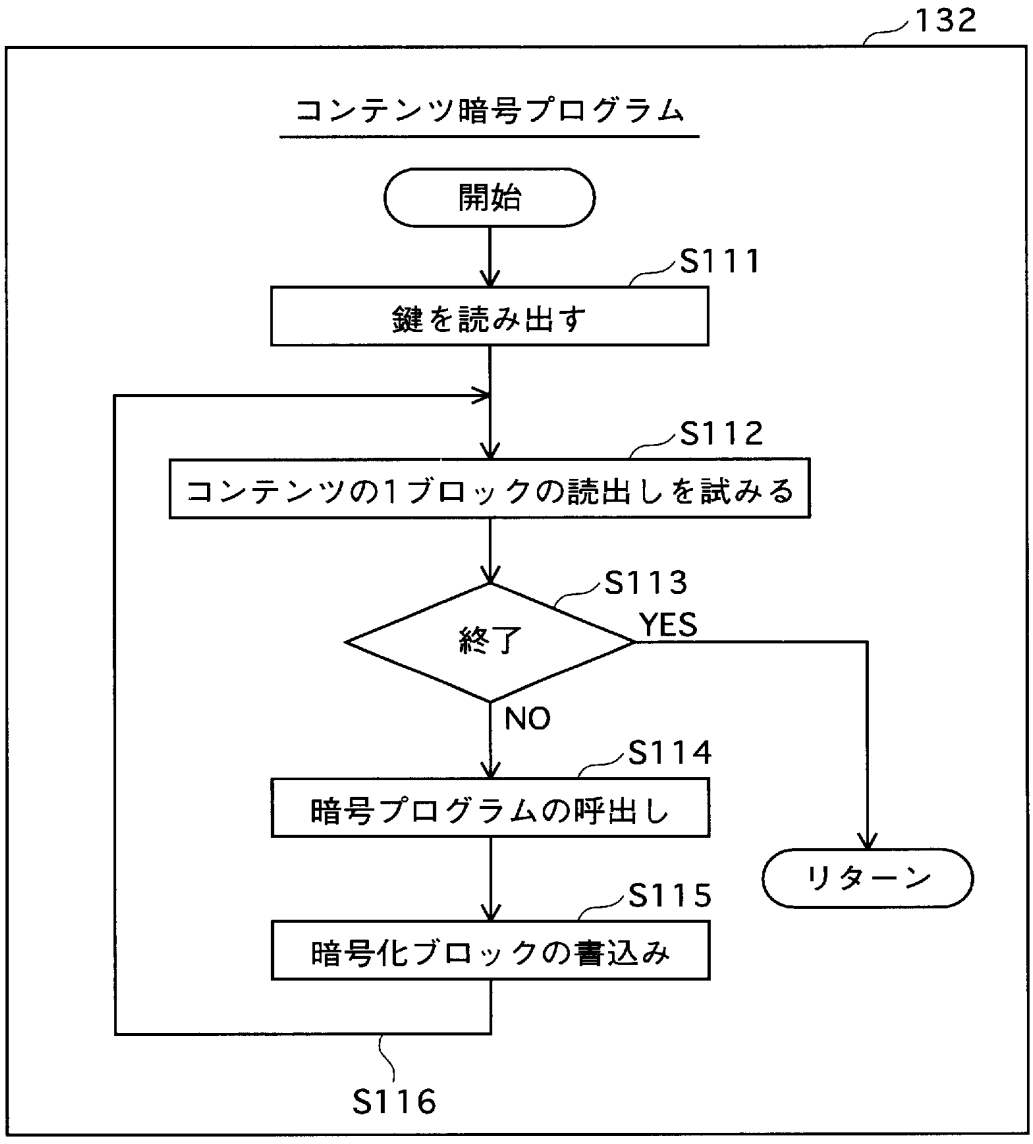
[図2]


コンテンツサーバ装置
100
マイクロプロセッサ
101
ハードディスク部
102
メモリ部
103
入力制御部
104
表示制御部
105
通信ユニット
106
キーボード
107
モニタ
108
コンテンツ
120
鍵
123
暗号化コンテンツ
126
コンテンツ
121
鍵
124
暗号化コンテンツ
127
コンテンツ
122
鍵
125
暗号化コンテンツ
128
コンテンツ配信プログラム
131
コンテンツ暗号プログラム
132
暗号プログラム
133
送信プログラム
134

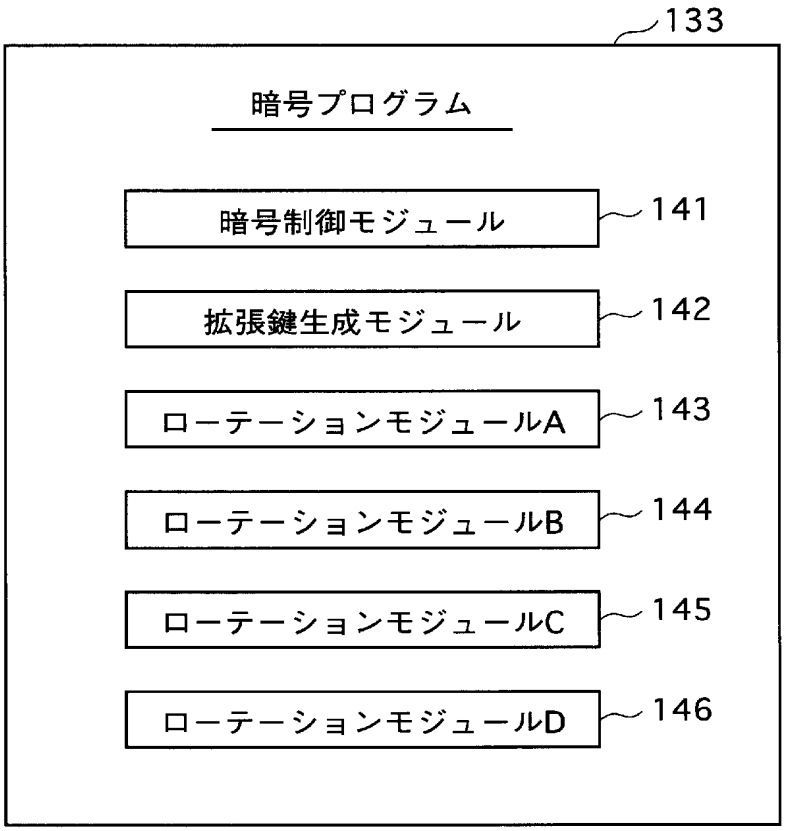
[図3]


131
コンテンツ配信プログラム
開始
S101
コンテンツの指定の受け付け
S102
配信先の指定の受け付け
S103
コンテンツ暗号プログラムの呼出し
S104
暗号化コンテンツの配信先への送信
終了

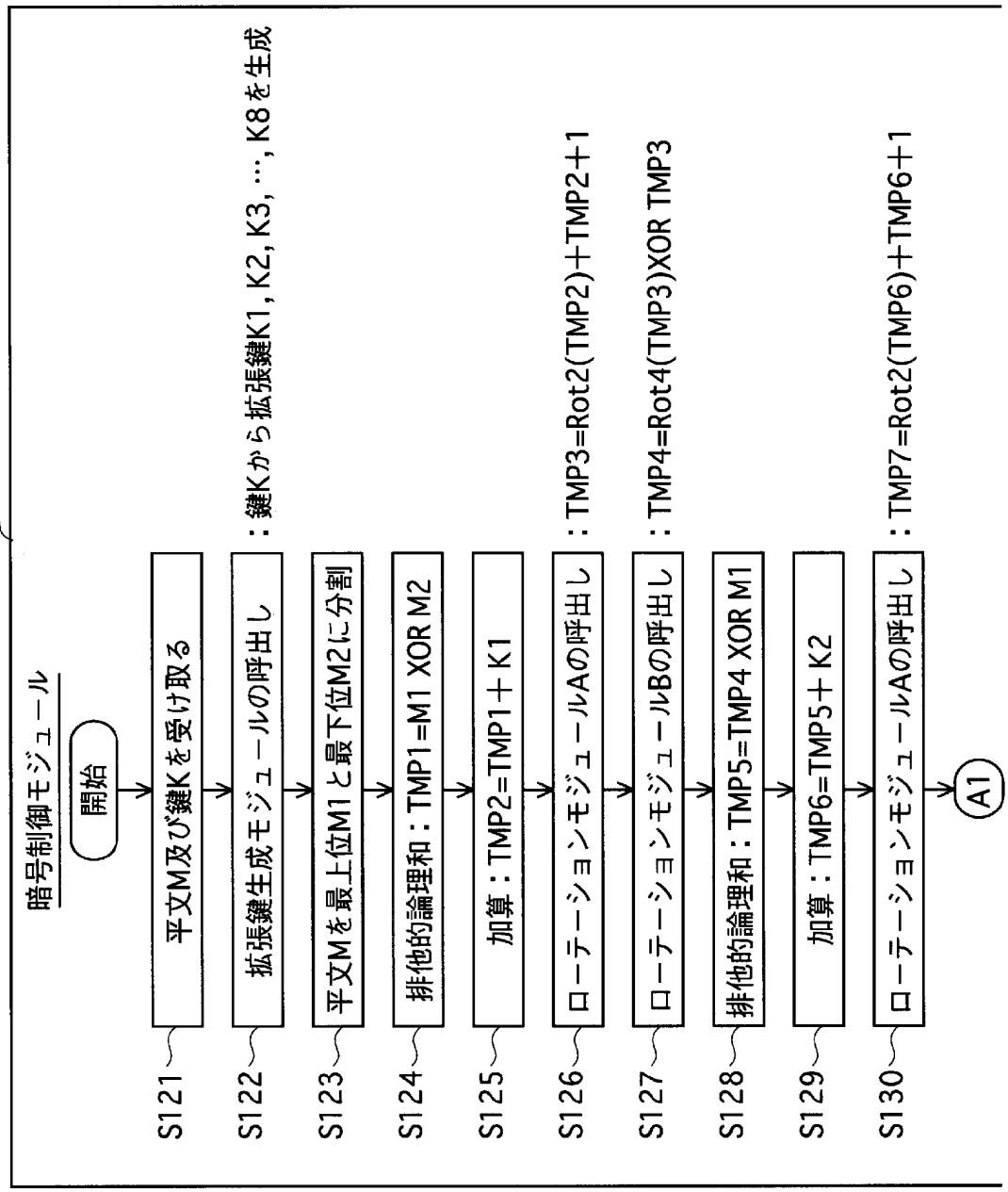
[図4]


132
コンテンツ暗号プログラム
開始
S111
鍵を読み出す
S112
コンテンツの1ブロックの読出しを試みる
S113
終了
YES
NO
S114
暗号プログラムの呼出し
リターン
S115
暗号化ブロックの書込み
S116

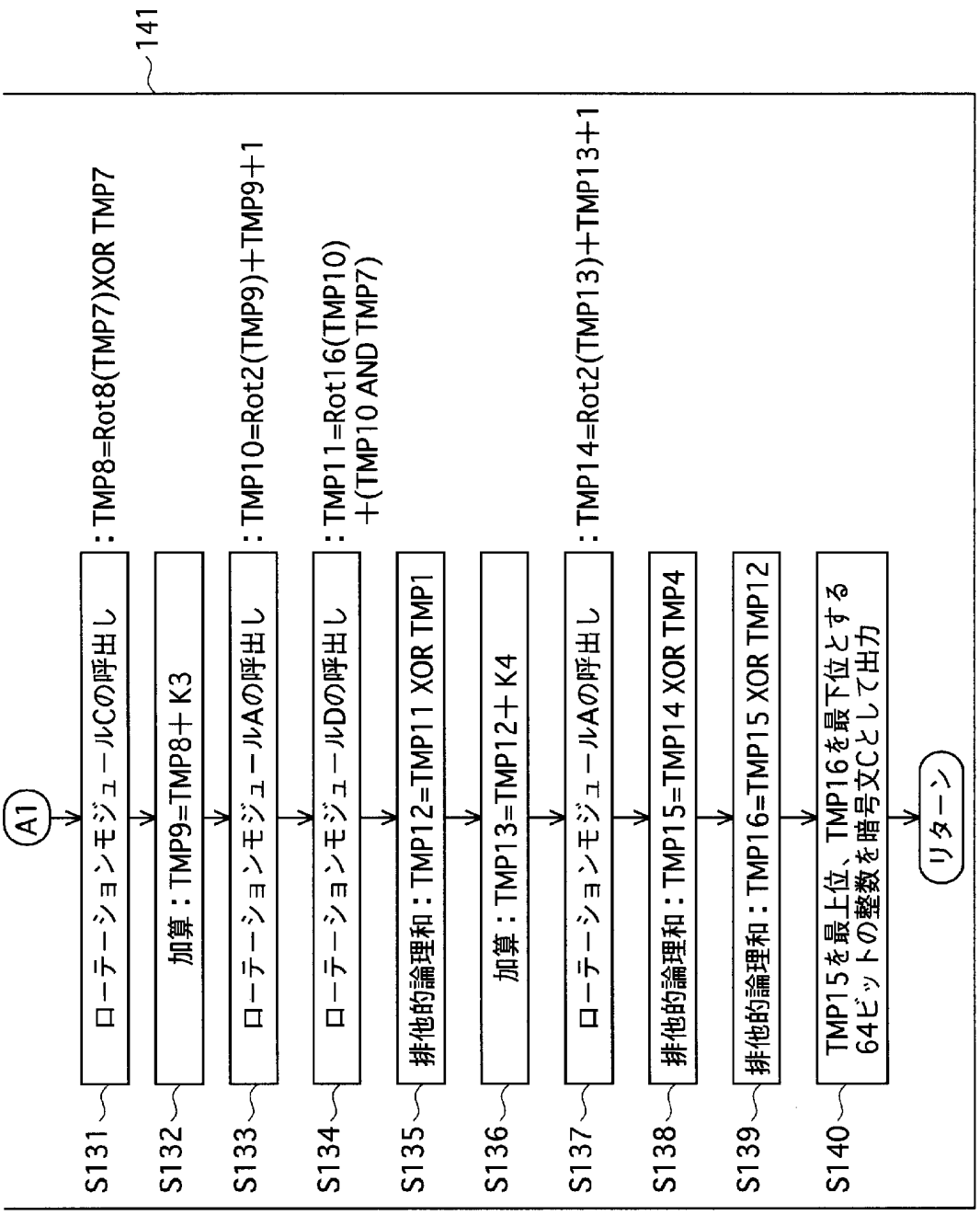
[図5]


133
暗号プログラム
暗号制御モジュール
141
拡張鍵生成モジュール
142
ローテーションモジュールA
143
ローテーションモジュールB
144
ローテーションモジュールC
145
ローテーションモジュールD
146

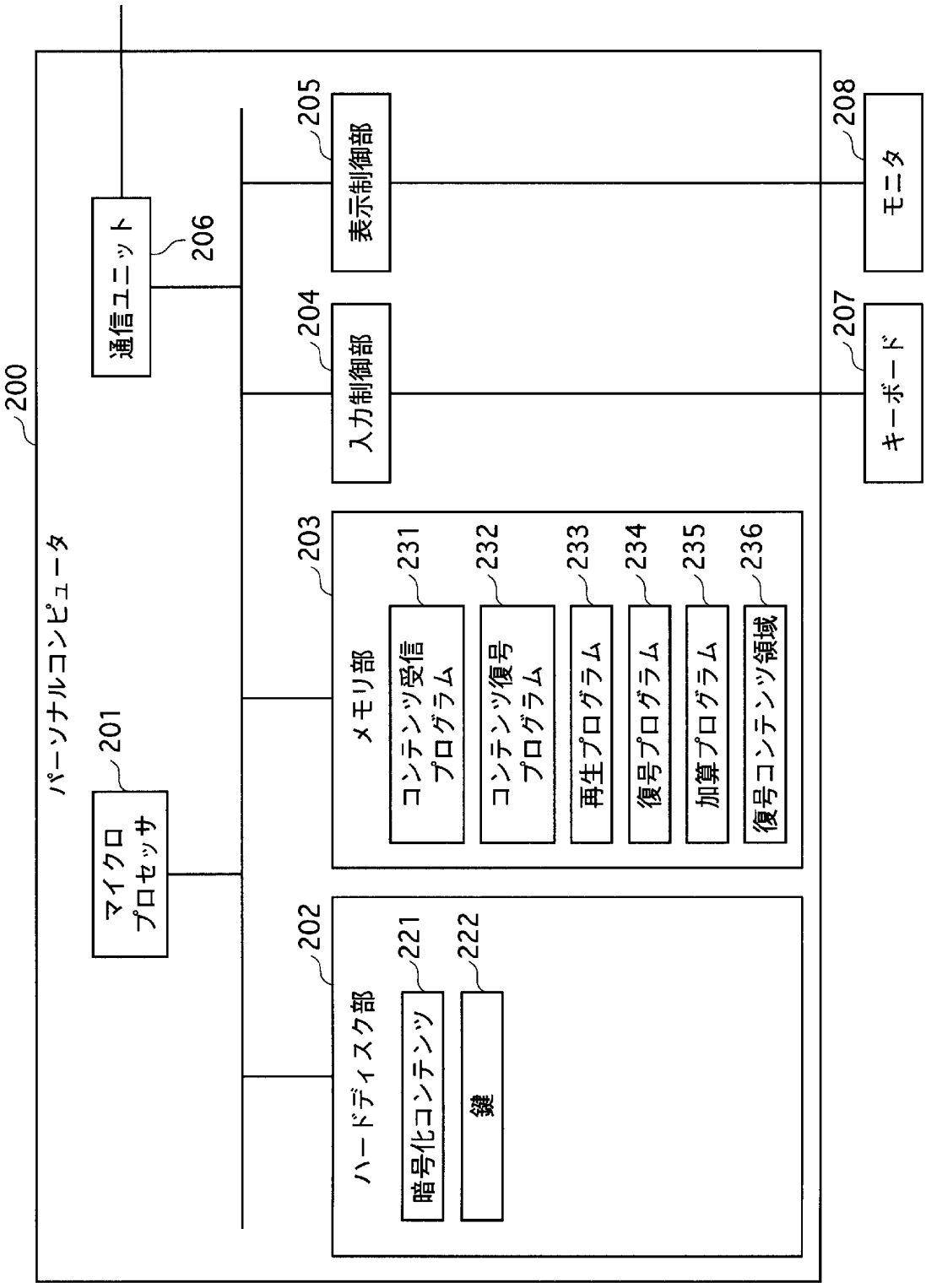
[図6]


141
暗号制御モジュール
開始
S121
平文M及び鍵Kを受け取る
S122
拡張鍵生成モジュールの呼出し
：鍵Kから拡張鍵K1, K2, K3, …, K8を生成
S123
平文Mを最上位M1と最下位M2に分割
S124
排他的論理和：TMP1=M1 XOR M2
S125
加算：TMP2=TMP1＋K1
S126
ローテーションモジュールAの呼出し
：TMP3=Rot2(TMP2)+TMP2+1
S127
ローテーションモジュールBの呼出し
：TMP4=Rot4(TMP3)XOR TMP3
S128
排他的論理和：TMP5=TMP4 XOR M1
S129
加算：TMP6=TMP5＋K2
S130
ローテーションモジュールAの呼出し
：TMP7=Rot2(TMP6)+TMP6+1
A1

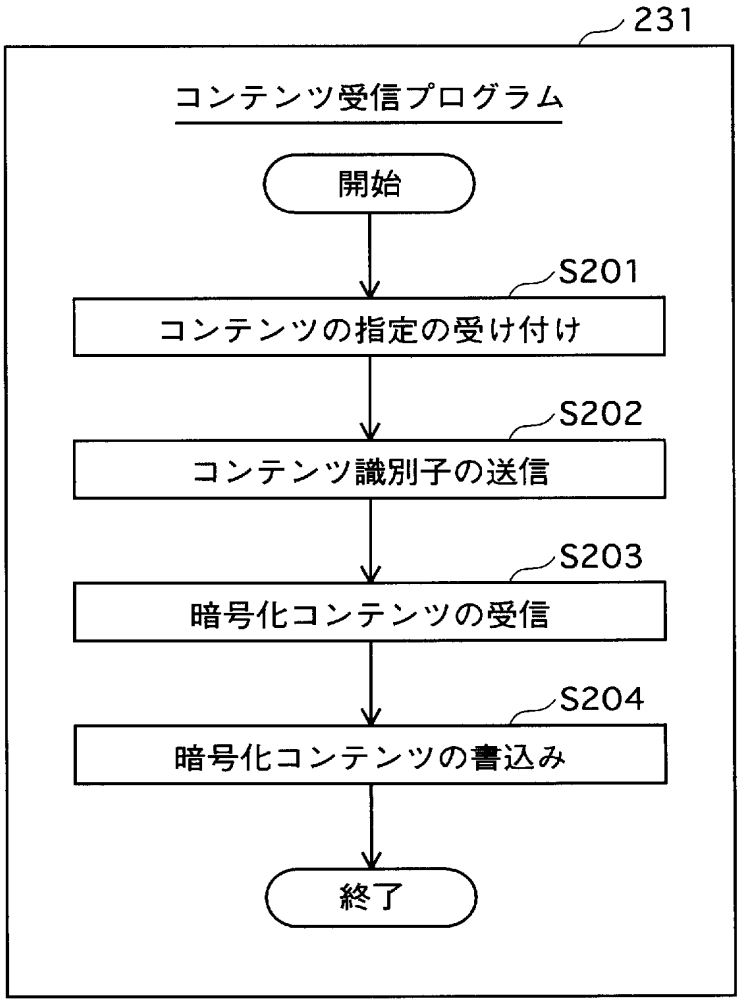
[図7]


141
A1
S131
ローテーションモジュールCの呼出し
: TMP8=Rot8(TMP7)XOR TMP7
S132
加算：TMP9=TMP8+ K3
S133
ローテーションモジュールAの呼出し
: TMP10=Rot2(TMP9)+TMP9+1
S134
ローテーションモジュールDの呼出し
: TMP11=Rot16(TMP10)
+(TMP10 AND TMP7)
S135
排他的論理和：TMP12=TMP11 XOR TMP1
S136
加算：TMP13=TMP12+ K4
S137
ローテーションモジュールAの呼出し
: TMP14=Rot2(TMP13)+TMP13+1
S138
排他的論理和：TMP15=TMP14 XOR TMP4
S139
排他的論理和：TMP16=TMP15 XOR TMP12
S140
TMP15を最上位、TMP16を最下位とする
64ビットの整数を暗号文Cとして出力
リターン

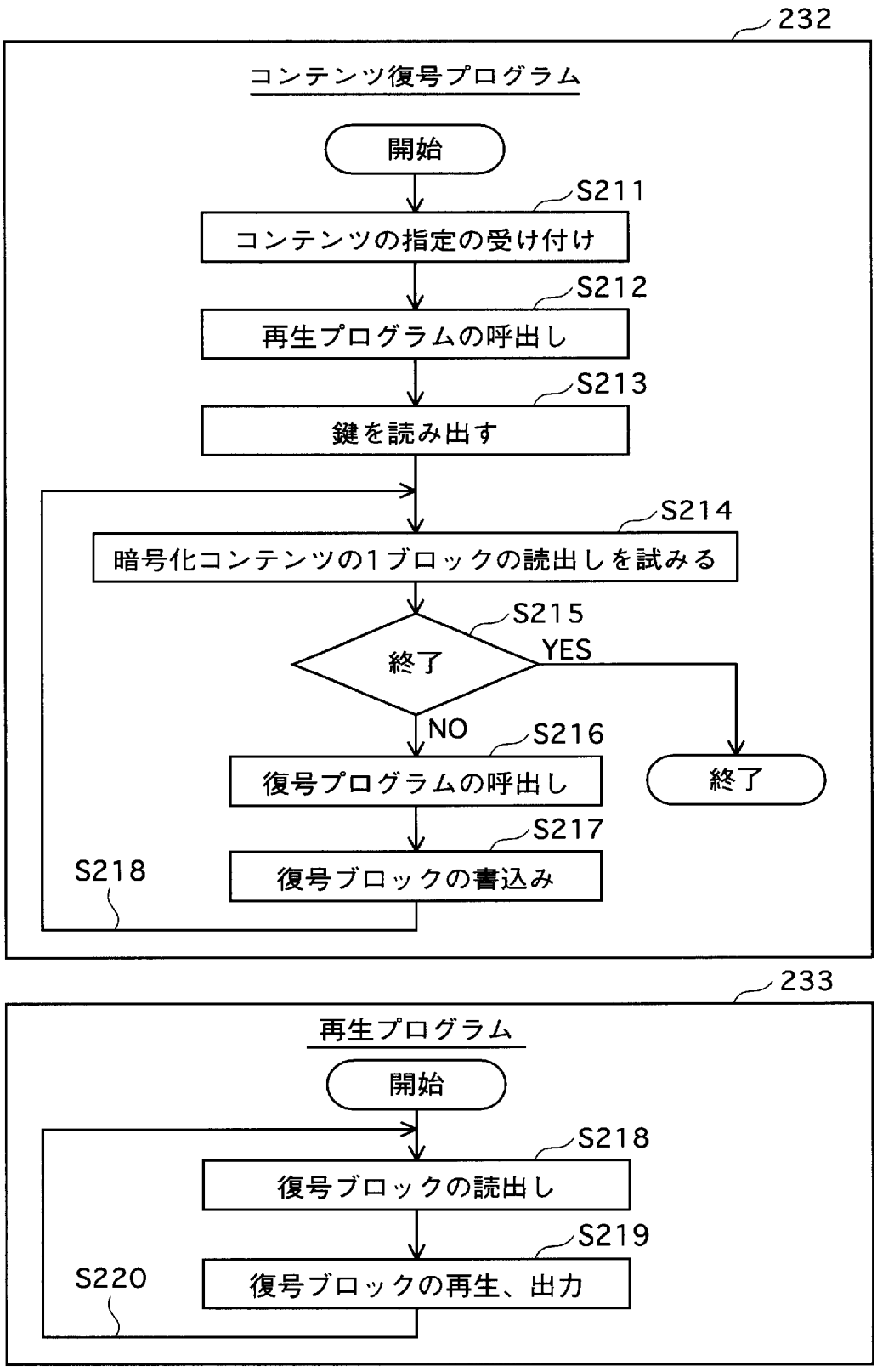
[図8]


200
パーソナルコンピュータ
201
マイクロプロセッサ
202
ハードディスク部
221
暗号化コンテンツ
222
鍵
203
メモリ部
231
コンテンツ受信プログラム
232
コンテンツ復号プログラム
233
再生プログラム
234
復号プログラム
235
加算プログラム
236
復号コンテンツ領域
204
入力制御部
205
表示制御部
206
通信ユニット
207
キーボード
208
モニタ

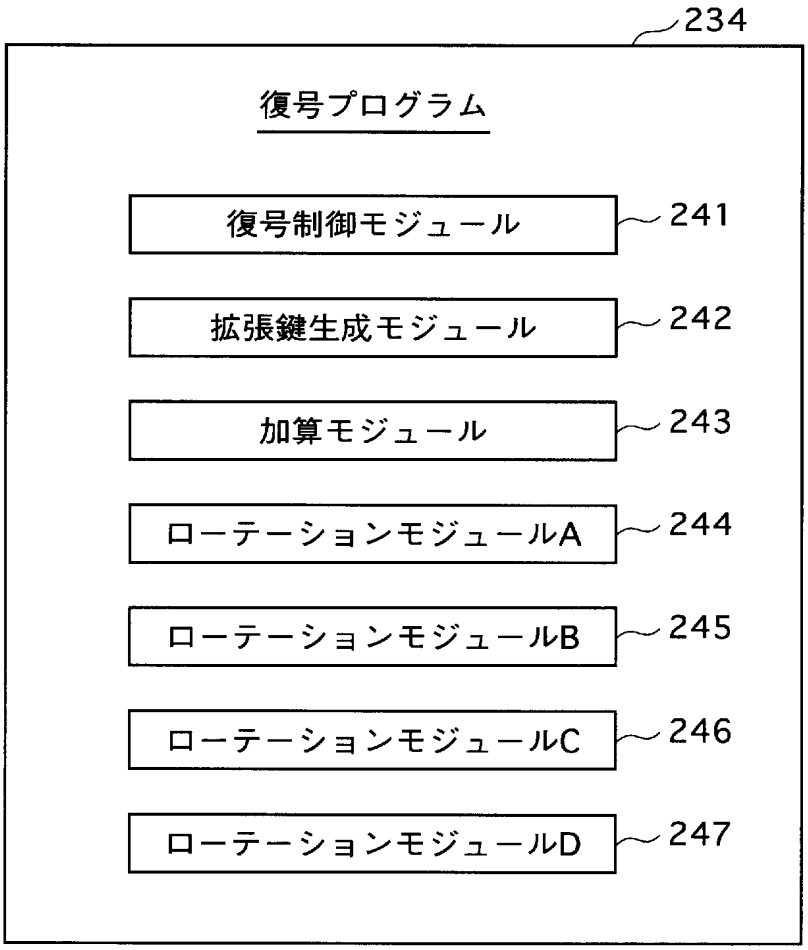
[図9]


231
コンテンツ受信プログラム
開始
S201
コンテンツの指定の受け付け
S202
コンテンツ識別子の送信
S203
暗号化コンテンツの受信
S204
暗号化コンテンツの書込み
終了

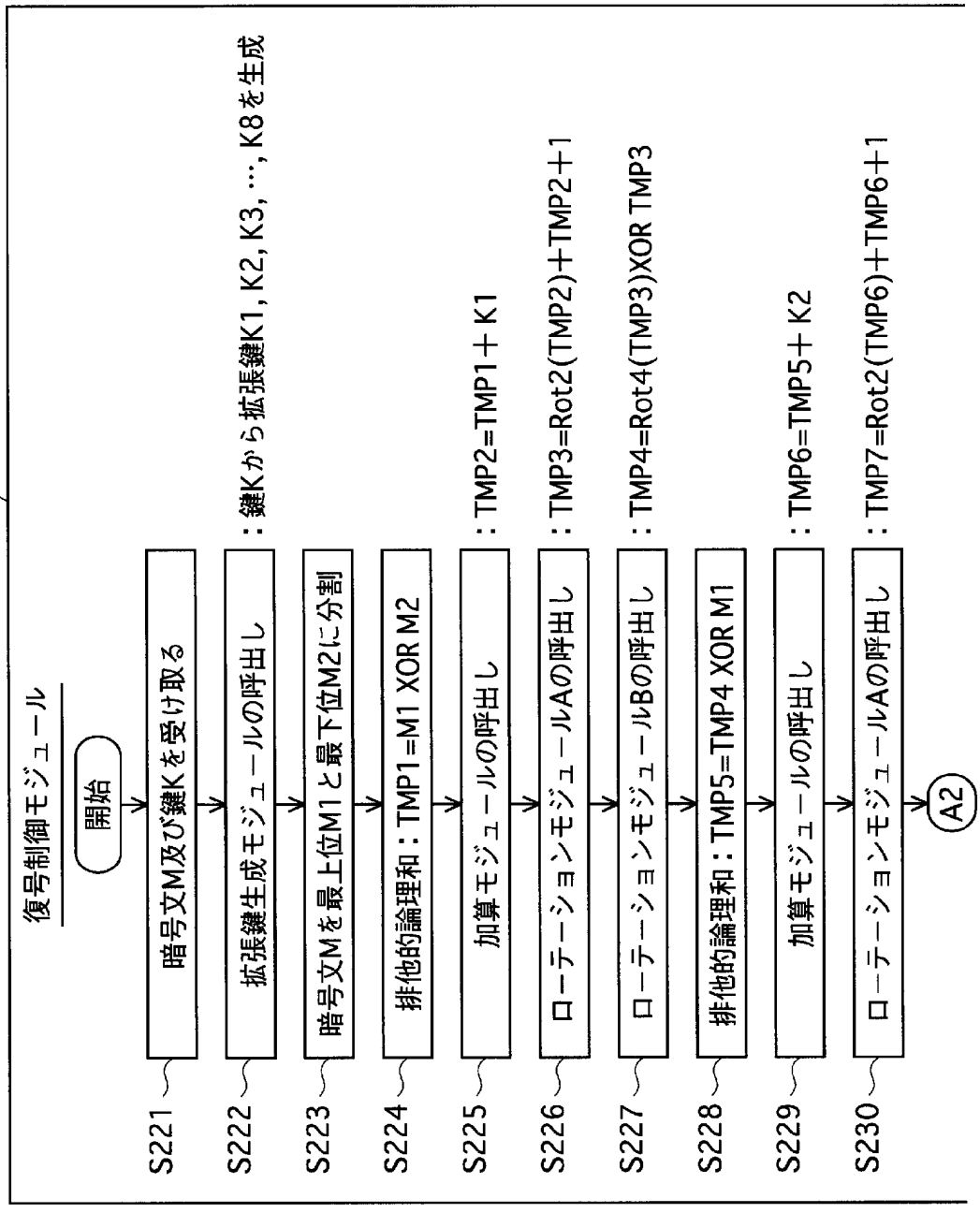
[図10]


232
コンテンツ復号プログラム
開始
S211
コンテンツの指定の受け付け
S212
再生プログラムの呼出し
S213
鍵を読み出す
S214
暗号化コンテンツの1ブロックの読出しを試みる
S215
終了
YES
NO
S216
復号プログラムの呼出し
終了
S217
復号ブロックの書込み
S218
233
再生プログラム
開始
S218
復号ブロックの読出し
S219
復号ブロックの再生、出力
S220

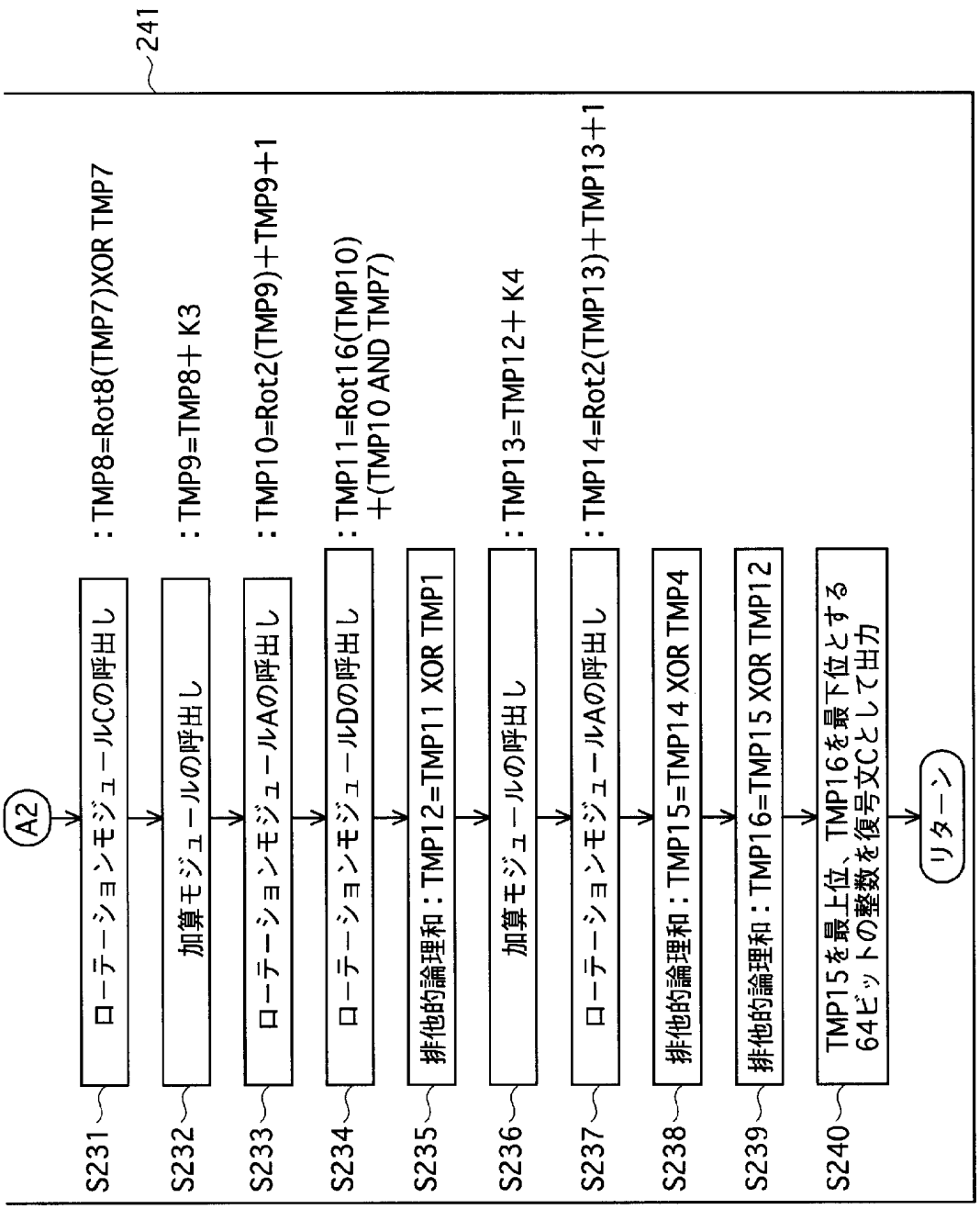
[図11]


234
復号プログラム
復号制御モジュール
241
拡張鍵生成モジュール
242
加算モジュール
243
ローテーションモジュールA
244
ローテーションモジュールB
245
ローテーションモジュールC
246
ローテーションモジュールD
247

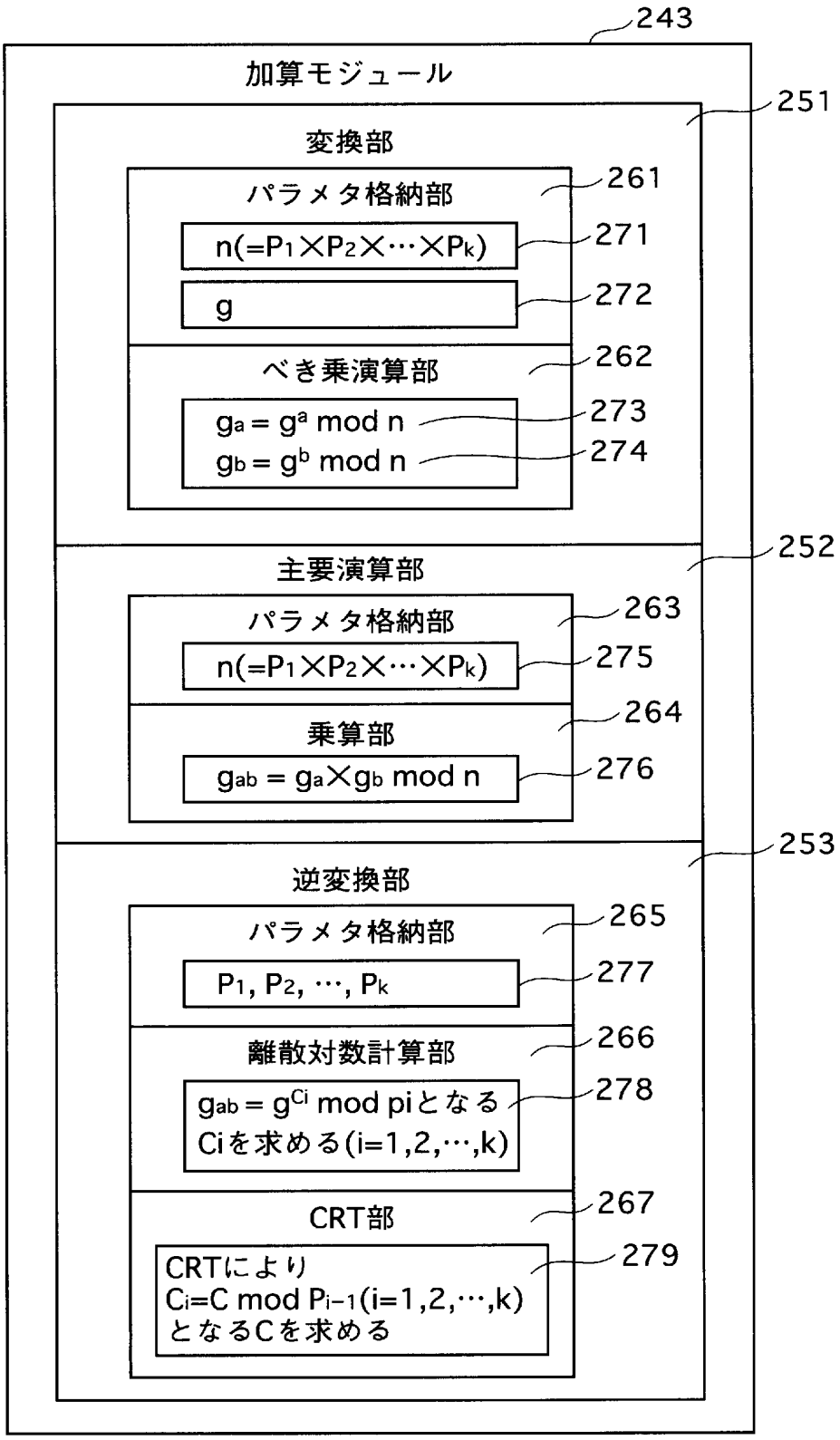
[図12]


241
復号制御モジュール
開始
S221
暗号文M及び鍵Kを受け取る
S222
拡張鍵生成モジュールの呼出し
：鍵Kから拡張鍵K1, K2, K3, …, K8を生成
S223
暗号文Mを最上位M1と最下位M2に分割
S224
排他的論理和：TMP1=M1 XOR M2
S225
加算モジュールの呼出し
：TMP2=TMP1＋K1
S226
ローテーションモジュールAの呼出し
：TMP3=Rot2(TMP2)+TMP2+1
S227
ローテーションモジュールBの呼出し
：TMP4=Rot4(TMP3)XOR TMP3
S228
排他的論理和：TMP5=TMP4 XOR M1
S229
加算モジュールの呼出し
：TMP6=TMP5＋K2
S230
ローテーションモジュールAの呼出し
：TMP7=Rot2(TMP6)+TMP6+1
A2

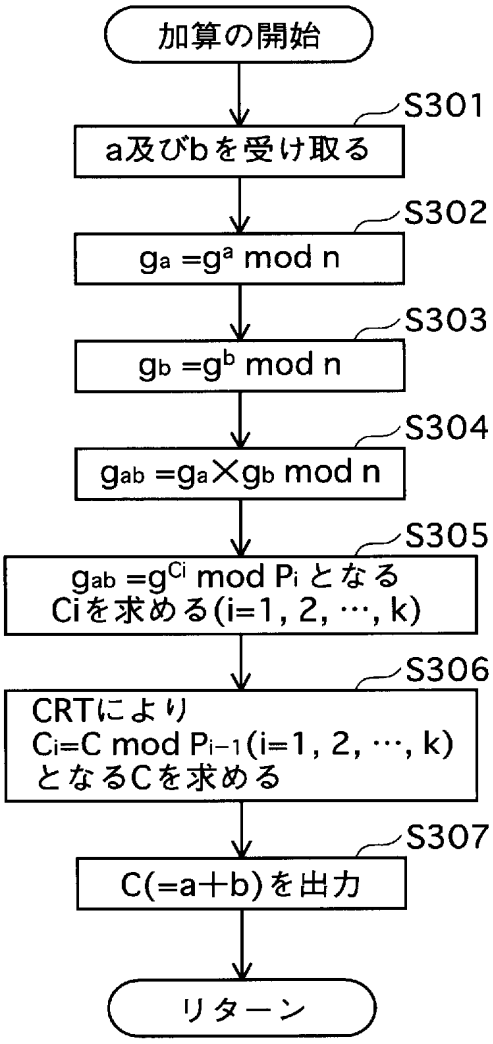
[図13]


241
A2
S231
ローテーションモジュールCの呼出し
: TMP8=Rot8(TMP7)XOR TMP7
S232
加算モジュールの呼出し
: TMP9=TMP8+ K3
S233
ローテーションモジュールAの呼出し
: TMP10=Rot2(TMP9)+TMP9+1
S234
ローテーションモジュールDの呼出し
: TMP11=Rot16(TMP10)
+(TMP10 AND TMP7)
S235
排他的論理和：TMP12=TMP11 XOR TMP1
S236
加算モジュールの呼出し
: TMP13=TMP12+ K4
S237
ローテーションモジュールAの呼出し
: TMP14=Rot2(TMP13)+TMP13+1
S238
排他的論理和：TMP15=TMP14 XOR TMP4
S239
排他的論理和：TMP16=TMP15 XOR TMP12
S240
TMP15を最上位、TMP16を最下位とする
64ビットの整数を復号文Cとして出力
リターン

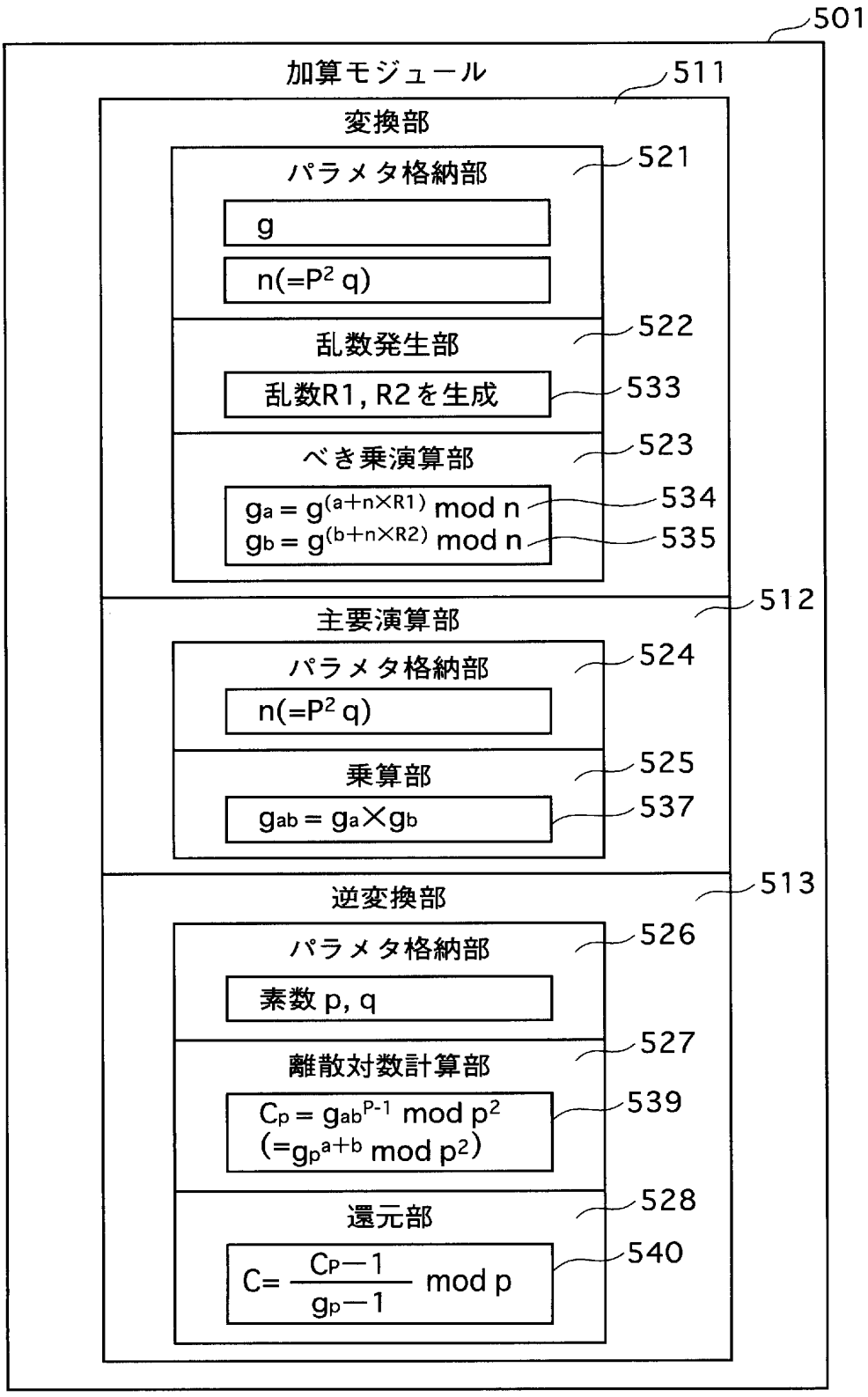
[図14]


243
加算モジュール
251
変換部
261
パラメタ格納部
n(=P1×P2×…×Pk)
271
g
272
262
べき乗演算部
ga = g^a mod n
273
gb = g^b mod n
274
252
主要演算部
263
パラメタ格納部
n(=P1×P2×…×Pk)
275
264
乗算部
gab = ga×gb mod n
276
253
逆変換部
265
パラメタ格納部
P1, P2, …, Pk
277
266
離散対数計算部
gab = g^Ci mod piとなる
Ciを求める(i=1,2,…,k)
278
267
CRT部
CRTにより
Ci=C mod Pi-1(i=1,2,…,k)
となるCを求める
279

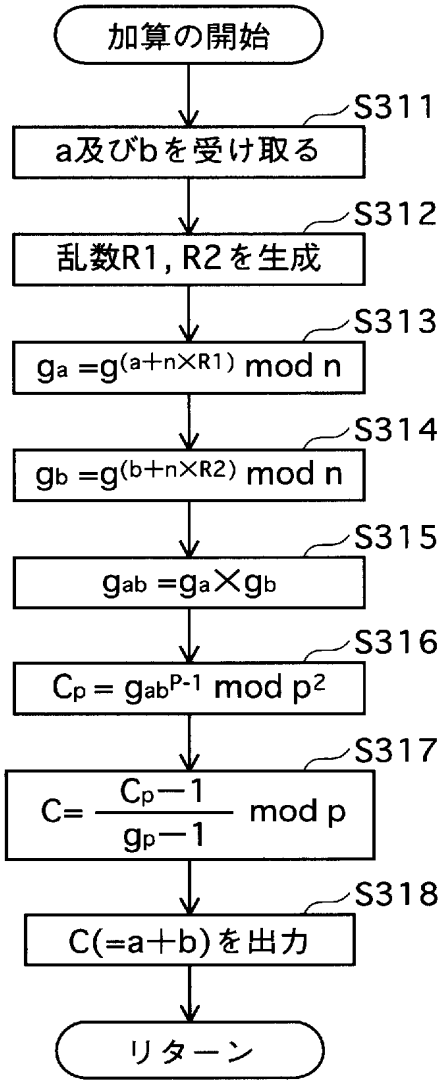
[図15]


加算の開始
S301
a及びbを受け取る
S302
$g_a = g^a \bmod n$
S303
$g_b = g^b \bmod n$
S304
$g_{ab} = g_a \times g_b \bmod n$
S305
$g_{ab} = g^{Ci} \bmod P_i$ となる
Ciを求める(i=1, 2, …, k)
S306
CRTにより
$C_i = C \bmod P_{i-1}$ (i=1, 2, …, k)
となるCを求める
S307
C(=a+b)を出力
リターン

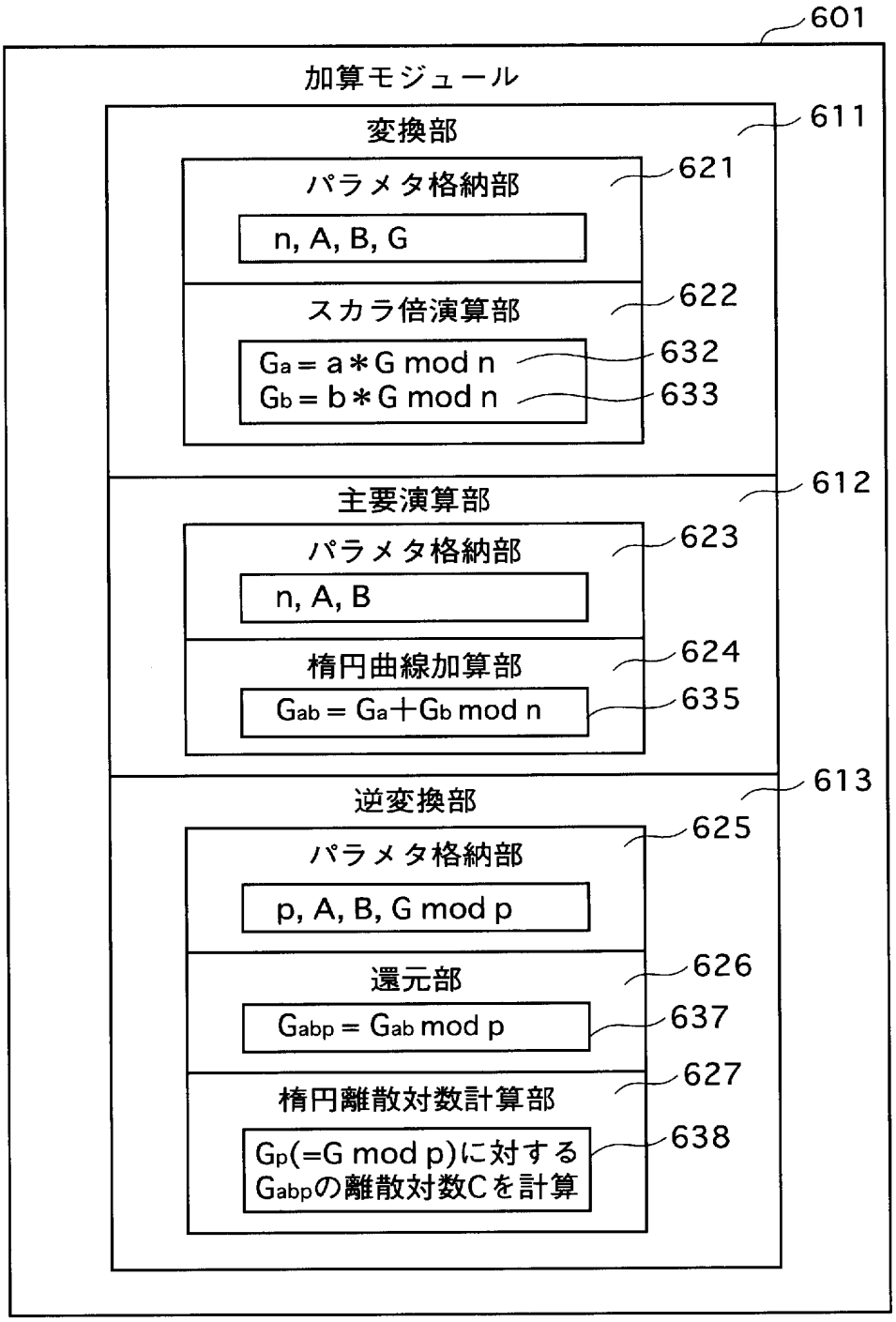
[図16]


501
加算モジュール
511
変換部
521
パラメタ格納部
g
n(=P2 q)
522
乱数発生部
乱数R1, R2を生成
533
523
べき乗演算部
ga = g(a+n×R1) mod n
534
gb = g(b+n×R2) mod n
535
512
主要演算部
524
パラメタ格納部
n(=P2 q)
525
乗算部
gab = ga×gb
537
513
逆変換部
526
パラメタ格納部
素数 p, q
527
離散対数計算部
Cp = gabP-1 mod p2
(=gpa+b mod p2)
539
528
還元部
C= Cp−1 / gp−1 mod p
540

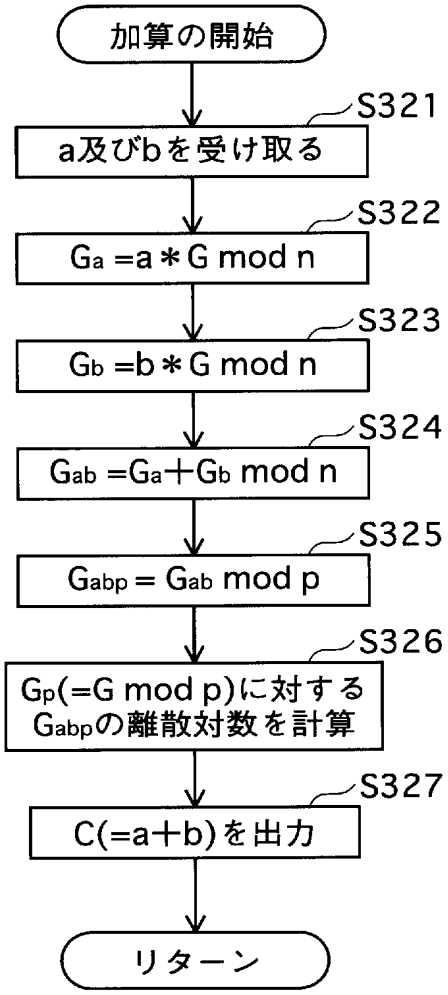
[図17]


加算の開始
S311
a及びbを受け取る
S312
乱数R1, R2を生成
S313
$g_a = g^{(a+n\times R1)} \bmod n$
S314
$g_b = g^{(b+n\times R2)} \bmod n$
S315
$g_{ab} = g_a \times g_b$
S316
$C_p = g_{ab}^{P-1} \bmod p^2$
S317
$C = \frac{C_p - 1}{g_p - 1} \bmod p$
S318
C(=a+b)を出力
リターン

[図18]


601
加算モジュール
611
変換部
621
パラメタ格納部
n, A, B, G
622
スカラ倍演算部
Ga = a * G mod n
632
Gb = b * G mod n
633
612
主要演算部
623
パラメタ格納部
n, A, B
624
楕円曲線加算部
Gab = Ga＋Gb mod n
635
613
逆変換部
625
パラメタ格納部
p, A, B, G mod p
626
還元部
Gabp = Gab mod p
637
627
楕円離散対数計算部
Gp(=G mod p)に対する
Gabpの離散対数Cを計算
638

[図19]


加算の開始
S321
a及びbを受け取る
S322
Ga =a＊G mod n
S323
Gb =b＊G mod n
S324
Gab =Ga＋Gb mod n
S325
Gabp = Gab mod p
S326
Gp(=G mod p)に対する
Gabpの離散対数を計算
S327
C(=a＋b)を出力
リターン

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/005136

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G09C1/00, G06F7/50

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G09C1/00, G06F7/50

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Toroku Jitsuyo Shinan Koho 1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 1999/001815 A1 (INTERTRUST, INC.), 14 January, 1999 (14.01.99), & AU 9879579 A & EP 988591 A1 & CN 1260055 A & JP 2002-514333 A & US 6668325 B1 7 Data Transformations	1-17,19-22
A	WO 2000/077597 A1 (CLOAKWARE CORP.), 21 December, 2000 (21.12.00), & AU 200053797 A & EP 1190292 A1 & US 6594761 B1 & US 2003/221121 A1 All pages	1-17,19-22

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 July, 2005 (29.07.05)	16 August, 2005 (16.08.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/005136

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SATO et al., "Data no Fugoka to Enzan no Henkan ni yoru Program no Nandokuka Shuho", The Institute of Electronics, Information and Communication Engineers Gijutsu Kenkyu Hokoku, Vol.102, No.743, pages 13 to 18, 19 March, 2003 (19.03.03), All pages	1-17,19-22
E,A	JP 2005-49925 A (Nara Insitute of Science and Technology), 24 February, 2005 (24.02.05), All pages (Family: none)	1-17,19-22

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/005136

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. [×] Claims Nos.: 18
because they relate to subject matter not required to be searched by this Authority, namely:
Claim 18 claims for a method for addition of an integer, i.e., mathematical theories.

2. [ ] Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. [ ] Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. [ ] As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. [ ] As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. [ ] As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. [ ] No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

[ ] The additional search fees were accompanied by the applicant's protest.

[ ] No protest accompanied the payment of additional search fees.

国際調査報告

国際出願番号 ＰＣＴ／ＪＰ２００５／００５１３６

Ａ． 発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.[7] G09C1/00, G06F7/50

Ｂ． 調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.[7] G09C1/00, G06F7/50

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００５年
日本国実用新案登録公報	１９９６－２００５年
日本国登録実用新案公報	１９９４－２００５年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ． 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	WO 1999/001815 A1 (INTERTRUST, INCORPORATED) 1999.01.14 & AU 9879579 A & EP 988591 A1 & CN 1260055 A & JP 2002-514333 A & US 6668325 B1 7 Data Transformations を参照	1-17, 19-22
A	WO 2000/077597 A1 (CLOAKWARE CORPORATION) 2000.12.21 & AU 200053797 A & EP 1190292 A1 & US 6594761 B1 & US 2003/221121 A1 全頁を参照	1-17, 19-22

☑ Ｃ欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日 ２９．０７．２００５	国際調査報告の発送日 16.8.2005
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） 中里 裕正 電話番号 ０３－３５８１－１１０１ 内線 ３５４６

５Ｓ ９３６４

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（２００４年１月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	佐藤 他，データの符号化と演算の変換によるプログラムの難読化手法，電子情報通信学会技術研究報告，Vol. 102 No. 743，p. 13-18，2003. 03. 19 全頁を参照	1-17, 19-22
ＥＡ	JP 2005-49925 A（国立大学法人 奈良先端科学技術大学院大学）2005. 02. 24 （ファミリなし）　全頁を参照	1-17, 19-22

国際調査報告

国際出願番号 ＰＣＴ／ＪＰ２００５／００５１３６

第Ⅱ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第8条第3項（ＰＣＴ17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☑ 請求の範囲 18 は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、
請求の範囲18は、整数を加算する方法を請求したものであるから、数学の理論に他ならない。

2．☐ 請求の範囲＿＿＿＿＿＿＿＿ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3．☐ 請求の範囲＿＿＿＿＿＿＿＿ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第3文の規定に従って記載されていない。

第Ⅲ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

1．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。